Multimedia Tools and Applications (2023) 82:43367–43419
https://doi.org/10.1007/s11042-023-15177-4

A robust semi-fragile watermarking system using Pseudo-Zernike moments and dual tree complex wavelet transform for social media content authentication

L. Agilandeeswari[1] · M. Prabukumar[1] · Farhan A Alenizi[2]

Received: 21 January 2022 / Revised: 13 July 2022 / Accepted: 27 March 2023 /
Published online: 13 April 2023

Abstract

With the growing use of mobile devices and Online Social Networks (OSNs), sharing digital content, especially digital images is extremely high as well as popular. This made us convenient to handle the ongoing COVID-19 crisis which has brought about years of change in the sharing of digital content online. On the other hand, the digital image processing tools which are powerful enough to make the perfect image duplication compromises the privacy of the transmitted digital content. Therefore, content authentication, proof of ownership, and integrity of digital images are considered crucial problems in the world of digital that can be accomplished by employing a digital watermarking technique. On contrary, watermarking issues are to triumph trade-offs among imperceptibility, robustness, and payload. However, most existing systems are unable to handle the problem of tamper detection and recovery in case of intentional and unintentional attacks concerning these trade-offs. Also, the existing system fails to withstand the geometrical attacks. To resolve the above shortcomings, this proposed work offers a new multi-biometric based semi-fragile watermarking system using Dual-Tree Complex Wavelet Transform (DTCWT) and pseudo-Zernike moments (PZM) for content authentication of social media data. In this research work, the DTCWT-based coefficients are used for achieving maximum embedding capacity. The Rotation and noise invariance properties of Pseudo Zernike moments make the system attain the highest level of robustness when compared to conventional watermarking systems. To achieve authentication and proof of identity, the watermarks of about four numbers are used for embedding as a replacement for a single watermark image in traditional systems. Among four watermarks, three are the biometric images namely Logo or unique image of the user, fingerprint biometric of the owner, and the metadata of the original media to be transmitted. In addition, to achieve the tamper localization property, the Pseudo Zernike moments of the original cover image are obtained as a feature vector and also embedded as a watermark. To attain a better level of security, each watermark is converted into Zernike moments, Arnold scrambled image, and SHA outputs respectively. Then, to sustain the trade-off among the watermarking parameters, the optimal embedding location is determined. Moreover, the watermarked image is also signed by the owner's other biometric namely digital signature, and converted into Public key matrix P_{km} and embedded onto the higher frequency subband namely, HL of the

Extended author information available on the last page of the article

1-level DWT. The proposed system also accomplishes a multi-level authentication, among that the first level is attained by the decryption of the extracted multiple watermark images with the help of the appropriate decryption mechanism which is followed by the comparison of the authentication key which is extracted using the key which is regenerated at the receiver's end. The simulation outcomes evident that the proposed system shows superior performance towards content authentication, to most remarkable intentional and unintentional attacks among the existing watermarking systems.

Keywords Content authentication · Cuckoo search optimization · Digital watermarking · Dual-tree complex wavelet transform · Intentional attacks · Pseudo-Zernike moments · Unintentional attacks

1 Introduction

ONLINE social media play an important role to connect people across the world through which every individual can connect with his/her friends and family, and share their information which is private using application software such as Microsoft Teams, Zoom, Google Meet, Duo, etc. Zoom app expanded from 10 M users in Dec'19 to 200 M in Mar'20 to 300 M in Apr'20. Since the Covid-19 pandemic lockdown has been activated all over the world, people started using online social networks such as WhatsApp, Twitter, Facebook, Instagram, LinkedIn, MySpace, Google+, Sina Weibo, Vkontakte, Mixi, and more for their communication not only for entertainment purpose but also basic needs. Multimedia data such as texts, images, audio, and videos are distributed easily over online social networks using the latest technology. However distributed data over online social media is often affected by malicious users that cause copyright violations, authenticity, ownership identity, and confidentiality issues. The discrepancy among the principles of online social media and copyright leads not only to misperception but also the susceptibility of users [18]. The authors recommended that Instagram should inform a better way to its users about the consequences when content is shared with a third party along with the agreement terms of its user by the copyright implementation strategy.

A recent report states that in a Design Thinking Challenge about sixty-eight people who are young helped those to have a deeper grasp of their experiences in electronic image-sharing, the harmful as well as helpful of images sharing repercussions on the mental health of adolescents, and safety, and also the interferences which are promising that makes young people take positive decisions in minimizing the dangers they face when exchanging photographs via technology devices [19]. Android App COVID Tracker attacks using ransomware virus. It forces a change in the unlock passwords AKA screen-lock attacks. Covid-19 tax payouts take the victim to fake government webpages and it Harvests all their financial and tax information. Two leading medical professionals Dr. Naresh Trehan, Medanta Medicity, and Dr. Devi Shetty from Narayana Health's attacked by fake news which leads to a nationwide emergency. Thus, there is an emergency in the requirement of data privacy on social media. An inclusive study of diverse privacy and safety and suspicions in social networking sites is presented in [46]. In addition, they also an emphasis on numerous extortions which ascend because of multimedia content sharing over online sites of social networks, and state-of-the-art defense solutions have been discussed to protect users of the social network from this kind of threats. Some social networks, like Twitter, MySpace, and Facebook always do not allow their users in disclosing their significant private information, but attackers may disclose their undisclosed information which is private. In 2005, the Sammy worm attacked MySpace, which exploited the susceptibilities in MySpace and transmitted very quickly. Similarly, in 2009, the Mikeyy worm attacked Twitter by replacing user data with some data which is unusable. In the same year, the Koobface worm attacked Facebook targeting it towards stealing users' important facts, namely the password of the user [39].

The rising use of social media by hackers cannot go ignored, according to the Internet Security Threat Report (ISTR) [54]. In 2015, such services were perverted into a source of unlawful online money-making through the use of malware and spam. Mark Zuckerberg, the CEO of Facebook, had his Pinterest and Twitter accounts hijacked recently, with the intruder attempting his LinkedIn password. The authors provided a collaborative analysis approach employing computational intelligence techniques to determine whether any online transmitted image has been edited or changed, and the material used to define which is accurate as in [25]. They investigated trending photographs using a collaborative search technique that took advantage of descriptive tags and user interaction histories. The authors of [64] provided a comprehensive overview of the current state of social media network security and reliability. They also addressed several open concerns and cutting-edge challenges in their research contribution.

[43] Proposes an adaptive LSB substitution picture steganography approach employing uncorrelated color space to address the privacy of graphic materials in online social networks (OSNs). To ensure the privacy of protected multimedia content on online social networks, a selective encryption strategy is utilized to lower the computational needs for large-size multimedia content. Only the most important parts of the cover media contents/any one of the color channels are encrypted [36].

After reviewing the aforementioned attack statistics, we concluded that the greatest route for an attacker to link cybercrime is through social media. To diminish these threats many researchers and industrialists have proposed various solutions that include watermarking [13, 35, 50, 65], steganalysis [34, 44, 58], and digital oblivion [22, 52] for protecting online social network users from hazards posed by multimedia data. To ensure the secure transmission of multimedia data over online social media various techniques such as cryptography [29–31, 45, 48], steganography [2, 23], and watermarking are used. Among these techniques, a watermarking-based system is suitable for all types of multimedia data transformation in a secured way over unsecured social media. Numerous research papers have been proposed to provide secure transformation of data using an image watermarking system over insecure networks. It is divided into two categories namely spatial domain and frequency domain approaches. Later one provides a robust and more complex system when compared to the former one [4–6, 8–10, 37, 63].

Some online social networks [41] use visible watermarking describes embedding the logo or text of the owner onto the cover contents that identifies multimedia content's ownership. This type of visible watermarking inclines to shield the data and is difficult to remove. After standard signal processing, fragile watermarks cannot be retrieved or validated. The hybrid of robustness and fragility defines a technique called semi-fragile watermarks. [44] Offers a unique approach for exchanging data which is on online social networks that minimize user privacy disclosure. To establish unified privacy regulations across numerous online social networks, it applies a public watermarking technology on multimedia material. They addressed the identity ownership issue by embedding multiple watermarks in place of the single, thus providing the additional security level and also condensed the requirements of bandwidth and storage mostly important for secure multimedia content applications on online social networks namely, education, E-health, driver's license/passport, secured E-Voting systems, digital cinema, and insurance companies. A modification of the Discrete Wavelet Transform (DWT) coefficient-based digital watermarking approach for online social networks is introduced by Thongkor et al. [56]. To protect cyberspace predominantly concentrating on information theft namely identity and credit card theft, thus cyber watermarking techniques are introduced by authors in [3].

When attackers damage the visible watermarks [57], it fails to offer authentication.

It is suggested to use a complete, hybrid, and reliable digital image watermarking. By using the most advantageous characteristics of an appropriate sub-band of DWT and the most optimal coefficients of DCT domain, color component, and appropriate embedding capacity, this method may establish a trade-off between imperceptibility, robustness, and embedding capacity. In order to attain particular parameters and reliable results for this study, multilateral examinations in a variety of scenarios have been tested [1].

A digital watermarking technique based on a rough Hadamard transform has been presented in [21]. The algorithm is comparable to the Hadamard transform, but the transform domain coefficients are multiplied, making it easier to precisely modify the quantization step size and improving the robustness that is readily available. Additionally, the technique makes use of various quantization step sizes in the RGB layers of color images via the variable step size theory to enhance invisibility.

By utilising the properties of the Slant transform, the suggested method [53] may directly extract the highest energy coefficient of the image block in the spatial domain. The coefficient is then quantized to contain the color digital watermark image after choosing the best quantization step using an adaptive quantization step technique. Additionally, the suggested method is compatible with colour digital photographs of various sizes in copyright protection and can adaptively select the watermark encoding type. The proposed method has demonstrated strong robustness and high real-time performance in the face of conventional image processing and geometric attacks, according to a substantial body of experimental data, which also confirms that it can satisfy the requirements of watermark invisibility and blind extraction.

An approach to watermarking that was suggested in [42] for patient identification and watermark integrity checking. In this method, the mid-frequencies of a discrete wavelet transform of the medical image have been merged with the patient's information fingerprint and its encrypted photography. The imperceptibility and robustness experimental findings show that the suggested solution preserves high quality watermarked images and a decent robustness against numerous common attacks.

[60] Introduces a durable digital image watermarking using Pseudo – Zernike moments, which uses image normalization to discover the geometrically invariant space. The normalized image's Pseudo Zernike moments are then figured out and from that, only the low-order moments are chosen for embedding. The authors of [11] presented ANiTW, a unique intelligent text watermarking technology. It hides an invisible watermark in Latin text-based information using an instance-based learning technique. Even if malicious individuals change or corrupt a section of the watermarked data, the system works flawlessly. But, this system fails to withstand all image forgery attacks. All the above existing systems, mostly detect the tampered region and classify it as malicious and non-malicious. Thus, the tampered recovery and determining the severity of the malicious or intentional attack is a challenging task. To avoid these downsides, not only the fragile watermarking systems [24] and also the semi-fragile-based watermarking systems which are both robust and fragile were developed. Most semi-fragile watermarking systems use Zernike moments-based feature vectors for tamper localization and recovery [40]. Some use edge features and Zernike features for the same [49]. Using semi-fragile watermarking and error-locating codes in

the DWT domain, we offer an approach for localizing image tampering in this paper. We demonstrate the advantages of employing control code error localization as an authentication function as well as its complexity by introducing several families of codes. In fact, to find image tampering, the proposed system in [33] demonstrate experimentally that error localization block codes are just as accurate as utilizing traditional error correcting codes (Reed-Solomon and BCH codes). However, the complexity of the relevant decoding algorithms is at least quadratic, making them unsuitable for some real-time applications. In order to address this issue, we develop error-control codes known as Error-Locating codes, where error localization is condensed to a single syndrome computation carried out using a minimal amount of binary operations.

Besides the above, to provide the balance among the semi-fragile watermarking systems' basic requirements, adaptivity is introduced in embedding and extraction. Even under unintended attacking situations, the encoded information cannot be accurately recovered when there is no adaptivity in the semi-fragile watermarking of images. Recently, the nature-inspired algorithms that are metaheuristics that mimic nature are now leading the techniques of digital watermarking for answering these issues either by finding an optimized location or embedding strength. In [27], the evolutionary algorithm namely the Genetic Algorithm is mainly used for acquiring the optimal embedding location for the insertion of a watermark. In [7], the adaptive robustness factor or scaling factor is calculated using a Firefly-based watermarking system. Recently, [8, 12] were used for determining the optimal embedding location and optimal scaling factor using a new optimization technique called cuckoo search optimization. Hence, as mentioned in [61], cuckoo search optimization performs well when equated to other metaheuristic algorithms.

1.1 Motivations

(i). From the survey, it is clear that the confidential multimedia data distributed over insecure social networks requires a higher level of authenticity as well as proof of ownership. Unauthenticated multimedia information needs to be further classified into intentional and unintentional attacks.

(ii). The visual quality of the semi-fragile watermarking systems is improved by determining the feature vectors of an image using the Zernike moments. Also, its robustness characteristic is improved with its rotation invariance.

(iii). To maintain the balance between the most important watermarking criteria, an adaptive embedding and extraction mechanism were introduced.

(iv). All these presented Zernike moments for tamper detection and recovery are vulnerable to high-density noise and have lesser embedding capacity. This motivates us to develop a Pseudo Zernike Moments-based watermarking system not only for the detection of tampers but also for their recovery.

The aforementioned literature review motivates us to create a nature-inspired image watermarking system that is both durable and safe using Cuckoo search optimization and DTCWT for proof of ownership and the authenticity of the multimedia information transmitted over insecure online social networks.

We have used the following terms in the proposed work: the Pseudo-Zernike Moments based Complex Wavelet Transform for a completely dissimilar purpose, such as embedding and extraction of confidential images on online social networks. In addition, using the available Dual-tree complex wavelet transform coefficients, our technique presents a new optimized system that identifies optimal scale coefficients used for watermarks embedding. In the proposed image work, the cover image is first undergoing DTCWT to obtain the transform coefficients. The invariant feature points are detected on the resultant coefficients of DTCWT using the Harris corner detector and the corner values are limited to 30. After that, use cuckoo search optimization is used to find the suitable block of pseudo-Zernike moments which is obtained on the feature points for the insertion of watermarks. The principal components of the multiple watermark images namely the unique logo image, owner's fingerprint, metadata, and Pseudo Zernike moments of the cover image are embedded onto the selected feature point's singular values which are obtained as an optimization output. Pseudo-Zernike moments' feature points are generally invariant to rotation and the detector namely the Harris corner helps to obtain the rotation and scaling invariant feature points; however, SVD provides translation or shift-invariant operations. Thus, to attain the RST property all these transformations are used. The watermarked image is the result of the inverse process of all of the preceding operations.

To improve the suitability of the suggested system for content authentication, various security levels are attained by authentication key generation that is obtained by combining watermarked image which is of zero attacks with the owner's digital signature. The resultant authentication key is then transmitted over a noisy channel which might be vulnerable to noise. It is then compared with the regenerated key at the receiver end with the help of the owner's digital signature and the received watermarked image (very likely assaulted). This authentication process can help the receiver to determine the authenticity of the received watermarked image if it is successful, the process of extraction has happened else, the received image is considered unauthenticated which might be tampered with either intentionally or unintentionally. The proposed system is based on semi-fragile because, the tamper detection and recovery happen for unintentional attacks namely noise additions, geometric attacks, and JPEG. On the other hand, based on the localization of tampered regions the severity of the intentional attack is determined. If the severity is greater than the threshold, the received watermarked image gets collapsed and thus gives no information. Thus the proposed technique achieves better visual quality with an average SSIM of a maximum of 0.9998 and a minimum of 0.8959 and the minimum and maximum PSNR values of 59 dB and 68 dB respectively. This proposed multi-biometric-based semi-fragile system is resistant to all types of geometric and some image forgery attacks that are highly correlated coefficients and stumpy bit error rates.

The following is a breakdown of the paper's structure. Section 2 details the existing systems review and contributions of our work. The preliminary notions are introduced in Section 3. The suggested semi-fragile multi-biometric watermarking scheme is detailed in Section 4. The experimental study and comparison of the suggested and conventional systems are covered in Sections 5 and 6. Section 7 concludes the article and deliberates the future directions.

2 Existing systems review and work contributions

This part expands on the existing systems' extensive analysis of the present challenges and also the contributions of our work.

2.1 Existing Systems Review and Challenges

The present systems' flaws were discovered as a result of the investigation mentioned above:

(i). None of the existing pseudo-Zernike moments based watermarking have been attempted for tamper detection and recovery.

(ii). Researchers have attempted a general watermarking system that is semi-fragile in the majority of existing techniques mainly to achieve tamper detection as well as recovery and image authenticity with limited attacks but not targeted towards online social media data. As the scope of transferring confidential information through social media increased nowadays and requires a higher level of authenticity and more image forgery needs to be classified.

(iii). The majority of contemporary digital image watermarking systems perform well for a variety of image processing operations and geometric distortion, but they are extremely vulnerable to image forgery assaults. Image forging attacks such as copy-move, image splicing, image flipping, and others decrease the detector's ability to identify the watermark.

(iv). None of the existing tamper detection and recovery systems dealt with Dual tree complex wavelet transform and optimal embedding location.

2.2 Work contributions

All the aforementioned factors are considered in this research work and devised a novel embedding and extraction approach:

(i). Introducing an efficient system that protects the multimedia data distributed over online social networks by providing authenticity, and proof of ownership using the concept of multi-biometrics and digital watermarking.

(ii). To cultivate a semi-fragile watermarking system that is both robust and secure against unauthorized access to or modification of multimedia data that is transmitted or uploaded over insecure online social networks.

(iii). In this approach, the basic semi-fragile watermarking systems are extended not only for localizing the tampered regions of various intentional attacks and also for their recovery based on the severity.

(iv). The meta-heuristic optimization technique is used to decide the embedding location which is optimal with the help of two objective functions, one depends on the maximum imperceptibility, Correlation coefficient, and capacity and the other depends on an average of a minimum of false-positive probabilities and false negative probabilities and squared Euclidean distance between the original cover image and watermarked image. Therefore, watermarking characteristics such as better visual quality, robustness, privacy, and embedding capacity are all achieved.

(v). The multi-biometric images as watermarks and the metadata and pseudo-Zernike moments of the cover images are embedded onto the pseudo-Zernike moment's singular values on the Harris feature points of DTCWT coefficients, which results in achieving robustness against noises, geometric, and other intentional attacks. Thus, one can attain better tamper detection and recovery.

3 Preliminary concepts

3.1 Pseudo-Zernike moments

Pseudo-Zernike moments (PZM) are due to Pseudo-Zernike polynomials and these are complex-valued polynomials which are orthogonal sets defined within the unit circle's interior $x^2+y^2>=1$ [33, 49]. The polynomials set is represented by $P_{nm}(x,y)\}$ and it is given as,

$$P_{nm}(x,y) = P_{nm}(p,\theta) = \ PZR_{nm}(p)exp(jm\theta) \tag{1}$$

where,

ρ sqrt(x^2+y^2), θ = tan−1(y/x).

n represents a non-negative integer,

m always has a value with condition |m| ≤ n and.

$PZR_{nm}(\rho)$ represents radial Pseudo-Zernike polynomial and it is expressed as,

$$PZR_{nm}(\rho) = \sum\nolimits_{s=0}^{n-|m|} \frac{(-1)^s(2n+1-s)!\rho^{n-s}}{s!(n+|m|+1-s)!(n-|m|-s)!} \tag{2}$$

An analog image *f(x,y)* can be decomposed using the above Pseudo-Zernike polynomial and it is expressed as,

$$f(x,y) = \sum\nolimits_{n=0}^{\infty} \sum\nolimits_{\{m:|m\leq n\}} AP_{nm}VP_{nm}(x,y) \tag{3}$$

where,

AP_{nm} represents *n* order pseudo-Zernike moments with *m* repetition and it is expressed as,

$$AP_{nm} = \frac{n+1}{\pi} \int\int_{x^2+y^2\leq 1} f(x,y)VP^*_{nm}(x,y)dxdy \tag{4}$$

In real-time, we mostly deal with digital images, but the above Pseudo Zernike moments AP_{nm} won't be directly applied, only its approximate version $\widehat{AP}_{nm}$ will be obtained as

$$\widehat{AP}_{nm} = \frac{n+1}{\pi} \sum\nolimits_{i=1}^{M} \sum\nolimits_{j=1}^{N} h_{nm}\left(x_i,y_j\right)f\left(x_i,y_j\right) \tag{5}$$

In Eq. (5), the *i* and *j* value are taken from the condition that $x_i^2+y_j^2 \leq 1$, and $h_{nm}(x_i,y_j)$ is given as

$$h_{nm}\left(x_i,y_j\right) = \int_{x_i-\frac{\Delta x}{2}}^{x_i+\frac{\Delta x}{2}} \int_{y_i-\frac{\Delta y}{2}}^{y_j+\frac{\Delta y}{2}} VP^*_{nm}(x,y)dxdy \tag{6}$$

where Δx = 2/M, Δy = 2/N.

Thus the Pseudo-Zernike moments used for discrete images in most of the literature are expressed PZM simply as,

$$PZM = \widehat{AP}_{nm} = \frac{n+1}{\pi} \sum_{i=1}^{M} \sum_{j=1}^{N} VP^{*}_{nm}\left(x_i, y_j\right) f\left(x_i, y_j\right) \Delta x \Delta y \tag{7}$$

The reconstruction of an image *f(x,y)'* from the obtained PZM is also possible due to its orthogonality and completeness property using the following expression,

$$f(x,y)' = \sum_{n=0}^{n_{max}} \sum_{m=-n}^{n} \widehat{AP}_{nm} VP_{nm}(x,y) \tag{8}$$

From [60], it is clear that when compared to Zernike and other existing moments, pseudo-Zernike moments are superior and various other moments particularly for image tamper detection and recovery mainly because of their properties, namely:

(i). More Feature representation capabilities: The capabilities of PZM in feature representation are found to be higher when compared to other moments namely Zernike moments because it affords more feature vectors as given in Table 1.

(ii). Robust against noise: PZM is orthogonal. As we know that the orthogonal moments are generally robust against noise, an image flipping or rotation does not affect their magnitudes,

(iii). Reconstruction ability: PZM can efficiently be used for image reconstruction.

(iv). Multilayer-based expression: Any given image outline can be represented in the form of moments which is low-order moments, whereas, the image details are represented using the high-order moments.

(v). Implementation ability: PZM can be implemented easily as its implementation is easier with the higher-order Pseudo-Zernike moments, unlike Hu moments.

Overall, PZM is a noble operator for image description. However, it is not invariance to scaling and translation directly, that can be attained with the help of image preprocessing via image normalization technology [51, 60]. Thus, invariance concerning scaling and translation is accomplished when an image is scaled to normal size after being translated to its centroid (Fig. 1).

For orders of about *n* numbers repetitions of about *m* numbers, the PZM and ZM values are depicted in Table 1. From the above table, both the pseudo-Zernike moments and Zernike moments can be expressed as lower-order and higher-order moments. From the Table, it is also evident that, for the same *n* number of orders, the *m* number of repetitions of PZM is more and thus has more numbers of feature vectors when compared to Zernike moments which in turn increase the embedding capacity. In particular, for applications namely information hiding, not all orders of moments are suitable [16, 55, 59] . Hence, the suitable orders as given in [60] are used. (i) The maximum orders that can be used are $n_{max} = 20$ and thus the corresponding number of feature vectors is given in Table 1 (ii) The moments with '*m*' number of repetitions whose value are the multiples of 4. i.e. 4i, for *i* = *0, 1, 2,3,4…p* are not suitable for reconstruction. The eligible PZM_E for any given image suits to perform information hiding is expressed based on the above conditions,

$$PZM_E = \{PZM\} \forall \begin{cases} n \le n_{max} \\ 0 \le m \le n \\ m \ne 4i \end{cases} \tag{9}$$

Table 1 Number of Pseudo-Zernike Moments (N_{PZM}) and Zernike Moments (N_{ZM})

Order *n*	Pseudo Zernike Moments (PZM) and Number of PZM	N_{PZM}	CN (M)	Zernike Moments (ZM) and Number of ZM	N_{ZM}	CN(*M*)
0	$PZM_{0,0}$	1	1	$ZM_{0,0}$	1	1
1	$PZM_{1,0,}$ $PZM_{1,1}$	2	3	$ZM_{1,1}$	1	2
2	$PZM_{2,0,}$ $PZM_{2,1,}$ $PZM_{2,2}$	3	6	$ZM_{2,0}$, $ZM_{2,2}$	2	4
3	$PZM_{3,0,}$ $PZM_{3,1,}$ $PZM_{3,2,}$ $PZM_{3,3}$	4	10	$ZM_{3,1}$, $ZM_{3,3}$	2	6
4	$PZM\ _{4,0,}$ $PZM\ _{4,1,}$ $PZM_{4,2,}$ $PZM_{4,3,}$ $PZM_{4,4}$	5	15	$ZM_{4,0}$, $ZM_{4,2,}$ $ZM_{4,4}$	3	9
5	$PZM_{5,0,}$ $PZM_{5,1,}$ $PZM_{5,2,}$ $PZM_{5,3,}$ $PZM_{5,4,}$ $PZM_{5,5}$	6	21	$ZM_{5,1}$, $ZM_{5,3,}$ $ZM_{5,5}$	3	12
6	$PZM_{6,0,}$ $PZM_{6,1,}$ $PZM_{6,2,}$ $PZM_{6,3,}$ $PZM_{6,4,}$ $PZM_{6,5,}$ $PZM_{6,6}$	7	28	$ZM_{6,0,}$ $ZM_{6,2,}$ $ZM_{6,4,}$ $ZM_{6,6}$	4	16
7	$PZM_{7,0,}$ $PZM_{7,1,}$ $PZM_{7,2,}$ $PZM_{7,3,}$ $PZM_{7,4,}$ $PZM_{7,5,}$ $PZM_{7,6,}$ $PZM_{7,7}$	8	36	$ZM_{7,1,}$ $ZM_{7,3,}$ $ZM_{7,5,}$ $ZM_{7,7}$	4	20
8	$PZM_{8,0,}$ $PZM_{8,1,}$ $PZM_{8,2,}$ $PZM_{8,3,}$ $PZM_{8,4,}$ $PZM_{8,5,}$ $PZM_{8,6,}$ $PZM_{8,7,}$ $PZM_{8,8}$	9	45	$ZM_{8,0,}$ $ZM_{8,2,}$ $ZM_{8,4,}$ $ZM_{8,6,}$ $ZM_{8,8}$	5	25
9	$PZM_{9,0,}$ $PZM_{9,1,}$ $PZM_{9,2,}$ $PZM_{9,3,}$ $PZM_{9,4,}$ $PZM_{9,5,}$ $PZM_{9,6,}$ $PZM_{9,7,}$ $PZM_{9,8,}$ $PZM_{9,9}$	10	55	$ZM_{9,1,}$ $ZM_{9,3,}$ $ZM_{9,5,}$ $ZM_{9,7,}$ $ZM_{9,9}$	5	30
10	$PZM_{10,0,}$ $PZM_{10,1,}$ $PZM_{10,2,}$ $PZM_{10,3,}$ $PZM_{10,4,}$ $PZM_{10,5,}$ $PZM_{10,6,}$ $PZM_{10,7,}$ $PZM_{10,8,}$ $PZM_{10,9,}$ $PZM_{10,10}$	11	66	$ZM_{10,0,}$ $ZM_{10,2,}$ $ZM_{10,4,}$ $ZM_{10,6,}$ $ZM_{10,8,}$ $ZM_{10,10}$	6	36
11	$PZM_{11,0,}$ $PZM_{11,1,}$ $PZM_{11,2,}$ $PZM_{11,3,}$ $PZM_{11,4,}$ $PZM_{11,5,}$ $PZM_{11,6,}$ $PZM_{11,7,}$ $PZM_{11,8,}$ $PZM_{11,9,}$ $PZM_{11,10,}$ $PZM_{11,11}$	12	78	$ZM_{11,1,}$ $ZM_{11,3,}$ $ZM_{11,5,}$ $ZM_{11,7,}$ $ZM_{11,9,}$ $ZM_{11,11}$	6	42
12	$PZM_{12,0,}$ $PZM_{12,1,}$ $PZM_{12,2,}$ $PZM_{12,3,}$ $PZM_{12,4,}$ $PZM_{12,5,}$ $PZM_{12,6,}$ $PZM_{12,7,}$ $PZM_{12,8,}$ $PZM_{12,9,}$ $PZM_{12,10,}$ $PZM_{12,11,}$ $PZM_{12,12}$	13	91	$ZM_{12,0,}$ $ZM_{12,2,}$ $ZM_{12,4,}$ $ZM_{12,6,}$ $ZM_{12,8,}$ $ZM_{12,10,}$ $ZM_{12,12}$	7	49
13	$PZM_{13,0,}$ $PZM_{13,1,}$ $PZM_{13,2,}$ $PZM_{13,3,}$ $PZM_{13,4,}$ $PZM_{13,5,}$ $PZM_{13,6,}$ $PZM_{13,7,}$ $PZM_{13,8,}$ $PZM_{13,9,}$ $PZM_{13,10,}$ $PZM_{13,11,}$ $PZM_{13,12,}$ $PZM_{13,13}$	14	105	$Z_{13,1,}$ $Z_{13,3,}$ $Z_{13,5,}$ $Z_{13,7,}$ $Z_{13,9,}$ $Z_{13,11,}$ $Z_{13,13}$	7	56
14	$PZM_{14,0,}$ $PZM_{14,1,}$ $PZM_{14,2,}$ $PZM_{14,3,}$ $PZM_{14,4,}$ $PZM_{14,5,}$ $PZM_{14,6,}$ $PZM_{14,7,}$ $PZM_{14,8,}$ $PZM_{14,9,}$ $PZM_{14,10,}$ $PZM_{14,11,}$ $PZM_{14,12,}$ $PZM_{14,13,}$ $PZM_{14.14}$	15	120	$Z_{14,0,}$ $Z_{14,2,}$ $Z_{14,4,}$ $Z_{14,6,}$ $Z_{14,8,}$ $Z_{14,10,}$ $Z_{14,12,}$ $Z_{14,13}$	8	64
15	$PZM_{15,0,}$ $PZM_{15,1,}$ $PZM_{15,2,}$ $PZM_{15,3,}$ $PZM_{15,4,}$ $PZM_{15,5,}$ $PZM_{15,6,}$ $PZM_{15,7,}$ $PZM_{15,8,}$ $PZM_{15,9,}$ $PZM_{15,10,}$ $PZM_{15,11,}$ $PZM_{15,12,}$ $PZM_{15,13,}$ $PZM_{15,14,}$ $PZM_{15,15}$	16	136	$Z_{15,1,}$ $Z_{15,3,}$ $Z_{15,5,}$ $Z_{15,7,}$ $Z_{15,9,}$ $Z_{15,11,}$ $Z_{15,13,}$ $Z_{15,15}$	8	72

Table 1 (continued)

Order n	Pseudo Zernike Moments (PZM) and Number of PZM	N$_{PZM}$	CN (M)	Zernike Moments (ZM) and Number of ZM	N$_{ZM}$	CN(M)
16	PZM$_{16,0}$, PZM$_{16,1}$, PZM$_{16,2}$, PZM$_{16,3}$, PZM$_{16,4}$, PZM$_{16,5}$, PZM$_{16,6}$, PZM$_{16,7}$, PZM$_{16,8}$, PZM$_{16,9}$, PZM$_{16,10}$, PZM$_{16,11}$, PZM$_{16,12}$, PZM$_{16,13}$, PZM$_{16,14}$, PZM$_{16,15}$, PZM$_{16,16}$	17	153	ZM$_{16,0}$, ZM$_{16,2}$, ZM$_{16,4}$, ZM$_{16,6}$, ZM$_{16,8}$, ZM$_{16,10}$, ZM$_{16,12,}$, ZM$_{16,14}$, ZM$_{16,16}$	9	81
17	PZM$_{17,0}$, PZM$_{17,1}$, PZM$_{17,2}$, PZM$_{17,3}$, PZM$_{17,4}$, PZM$_{17,5}$, PZM$_{17,6}$, PZM$_{17,7}$, PZM$_{17,8}$, PZM$_{17,9}$, PZM$_{17,10}$, PZMM$_{17,11}$, PZM$_{17,12}$, PZM$_{17,13}$, PZM$_{17,14}$, PZM$_{17,15}$, PZM$_{17,16}$, PZM$_{17,17}$	18	171	ZM$_{17,1}$, ZM$_{17,3}$, ZM$_{17,5}$, ZM$_{17,7}$, ZM$_{17,9}$, ZM$_{17,11}$, ZM$_{17,13}$, ZM$_{17,15}$, ZM$_{17,17}$	9	90
18	PZM$_{18,0}$, PZM$_{18,1}$, PZM$_{18,2}$, PZM$_{18,3}$, PZM$_{18,4}$, PZM$_{18,5}$, PZM$_{18,6}$, PZM$_{18,7}$, PZM$_{18,8}$, PZM$_{18,9}$, PZM$_{18,10}$, PZM$_{18,11}$, PZM$_{18,12}$, PZM$_{18,13}$, PZM$_{18,14}$, PZM$_{18,15}$, PZM$_{18,16}$, PZM$_{19,17}$, PZM$_{18,18}$	19	190	ZM$_{18,0}$, ZM$_{18,2}$, ZM$_{18,4}$, ZM$_{18,6}$, ZM$_{18,8}$, ZM$_{18,10}$, ZM$_{18,12}$, ZM$_{18,14}$, ZM$_{18,16}$, ZM$_{18,18}$	10	100
19	PZM$_{19,0}$, PZM$_{19,1}$, PZM$_{19,2}$, PZM$_{19,3}$, PZM$_{19,4}$, PZM$_{19,5}$, PZM$_{19,6}$, PZM$_{19,7}$, PZM$_{19,8}$, PZM$_{19,9}$, PZM$_{19,10}$, PZM$_{19,11}$, PZM$_{19,12}$, PZM$_{19,13}$, PZM$_{19,14}$, PZM$_{19,15}$, PZM$_{19,16}$, PZM$_{19,17}$, PZM$_{19,18}$, PZM$_{19,19}$	20	210	ZM$_{19,1}$, ZM$_{19,3}$, ZM$_{19,5}$, ZM$_{19,7}$, ZM$_{19,9}$, ZM$_{19,11}$, ZM$_{19,13}$, ZM$_{19,15}$, ZM$_{19,17}$, ZM$_{19,19}$	10	110
20	PZM$_{20,0}$, PZM$_{20,1}$, PZM$_{20,2}$, PZM$_{20,3}$, PZM$_{20,4}$, PZM$_{20,5}$, PZM$_{20,6}$, PZM$_{20,7}$, PZM$_{20,8}$, PZM$_{20,9}$, PZM$_{20,10}$, PZM$_{20,11}$, PZM$_{20,12}$, PZM$_{20,13}$, PZM$_{20,14}$, PZM$_{20,15}$, PZM$_{20,16}$, PZM$_{20,17}$, PZM$_{20,18}$, PZM$_{20,19}$, PZM$_{20,20}$	21	231	ZM$_{20,0}$, ZM$_{20,2}$, ZM$_{20,4}$, ZM$_{20,6}$, ZM$_{20,8}$, ZM$_{20,10}$, ZM$_{20,12}$, ZM$_{20,14}$, ZM$_{20,16}$, ZM$_{20,18}$, ZM$_{20,20}$	11	121

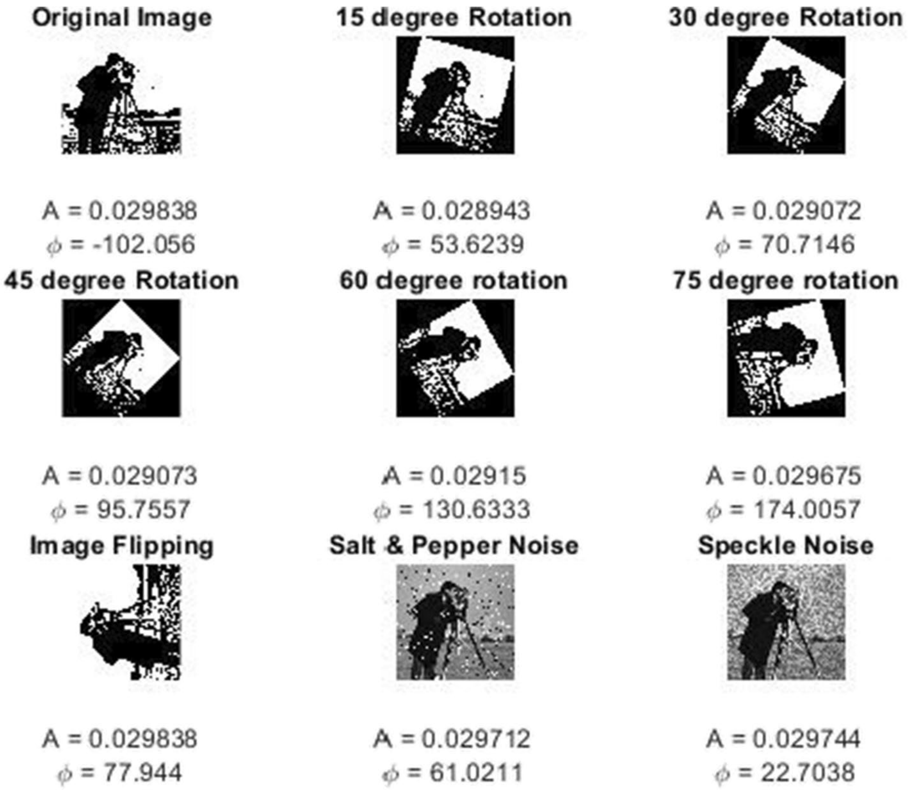


Fig. 1 Pseudo Zernike moments amplitude and phase values under various rotation angles and noises

The process of reconstruction is depicted in Fig. 2 for a ‘Lena’ test image of size 512*512, the reconstructed images are generated using the Eq. (8). It is obvious from the figure that the gross shape information is captured in the lower-order moments and the higher-order moments capture the high-frequency details. In our experiment, the 15th order of 136 moments shows a better trade-off between the detection accuracy and the computation time, and the same is demonstrated in the Section 4.

3.2 Dual–tree complex wavelet transform (DTCWT)

Transform domain techniques have a significant impact on various image processing applications. Various transforms are used to convert the spatial domain image into frequency coefficients, among those transforms discrete wavelet transform (DWT) performs better. The DWT transform, on the other hand, fails to maintain shift-invariance, resulting in large fluctuations when small shifts in the input data occur, there is a shift in the energy distribution between DWT coefficients, as well as poor directional selectivity for diagonal features [28]. Thus, DWT’s shortcomings can be addressed by Kingsbury who developed the Dual-Tree Complex Wavelet Transform. Its properties include shift-invariance, strong directional selectivity, perfect reconstruction, limited redundancy, and low computing complexity. It is derived from the DWT and Complex wavelet transformations (CWT) [28]. Here,

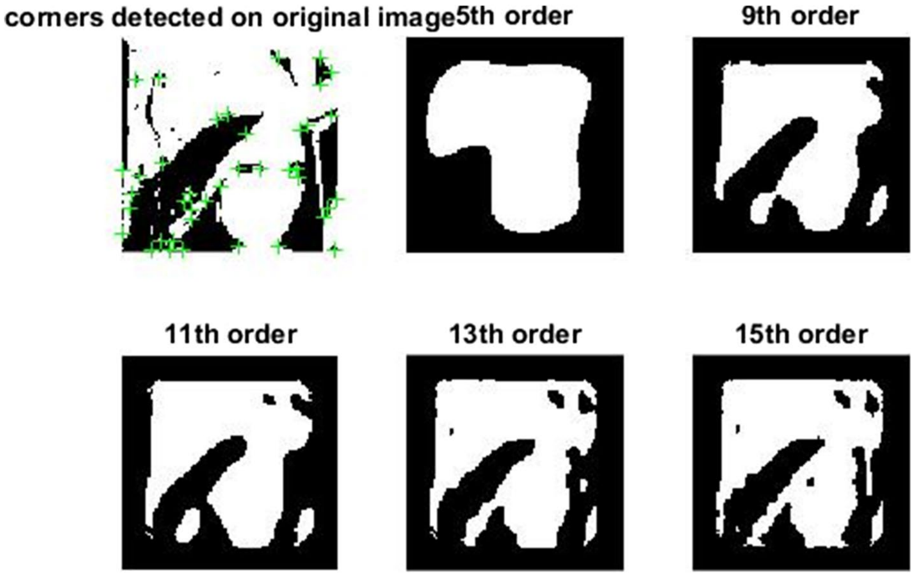


Fig. 2 Pseudo Zernike Moments and its reconstruction for 'Lena'

the complex coefficients are obtained by employing DTCWT on two real DWTs, each of which works on distinct filter sets for generating real as well as imaginary transform parts. To get two real signals, these parts are inverted namely real and imaginary using each of the two real DWTs' inverses. The final signal is then reconstructed by averaging these two signals [47].

Let *f(x,y)* input image gets decomposes into sequences of translations and dilations using DT-CWT using complex scaling function Φ(x,y) and thus results in complex wavelet functions of about six numbers $\psi^{\Theta}{}_{\mathrm{j,l}}$(x,y) and it is expressed as

$$f(x,y)=\sum_{l\in Z^2} S_{j0,l}\Phi_{j0,l}(x,y)+\sum_{\theta\epsilon\varnothing}\sum_{j\geq j_0}\sum_{l\in Z^2} C^{\theta}_{j,l}\psi^{\theta}_{j,l}(x,y) \tag{10}$$

In Eq. (10), $\theta\epsilon\{\pm 15^\circ,\pm 45^\circ,\pm 75^\circ\}$ represents the complex wavelet function's directionality, Z represents natural numbers, and j and l represent shifts and dilations, $C_{j,l}$ represents the wavelet coefficient which is complex with $\varphi_{j0,l}(x)=\varphi^{r}{}_{j0,l}(x)+\sqrt{-1\varphi^{i}_{j0,l}(x)}$ and $\psi_{j,l}(x)=\psi^{r}{}_{j,l}(x)+\sqrt{-1\psi^{i}_{j,l}}(x)$ where i and r represent the imaginary and real parts respectively.

Applying DTCWT on an image *f(x,y)* generates lower frequency subbands that are complex-valued of two numbers and higher frequency subbands that are also complex-valued of six numbers at every decomposition level. Each of these high-frequency subbands has a Θ direction which is unique at angles of ±15°, ±45°, and ± 75° [63].

For better understanding, the two complex valued low frequency coefficients are given as,

$$\begin{gathered}x(\lambda,L1,u,v)=Rl(x(\lambda,L1,u,v))+jImy(x(\lambda,L1,u,v))\\ x(\lambda,L2,u,v)=Rl(x(\lambda,L2,u,v))+jImy(x(\lambda,L2,u,v))\end{gathered}$$

and the six complex valued high frequency coefficients are expressed as,

$$x(\wedge, \theta, u, v) = Rl(x(\wedge, \theta, u, v)) + jImy(x(\wedge, \theta, u, v)) \tag{11}$$

thus,

Rl(.) and Imy(.) stands for real and imaginary parts respectively.

L1, and L2 represent low-frequency sub-bands.

$\wedge$ represents the level of decomposition, here it is 2.

ϴ represents direction of subband and its values are $\{-75, -45, -15, +15, +45, +75\}$.

u, v represents the location of the coefficient in each sub-band and its values vary as.

$0 \le u \le \frac{N}{2^{\wedge}} - 1$ and $0 \le v \le \frac{N}{2^{\wedge}} - 1$.

The DTCWT solves the problem which generally suffers by the DWT namely, lack of directionality, oscillations, shift variance, and aliasing on the 2D image. Figure 3 shows the application of DTCWT on test image '*lena*'. The DTCWT has several advantages, including shift-invariance, strong directional selectivity, flawless reconstruction, little redundancy, and low computing complexity, all of which make it appealing for developing efficient watermarking systems with a larger embedding domain.

Furthermore, the DTCWT has powerful perceptual features because of its good directional sensitivity at higher frequency sub-bands, resulting in increased embedded watermark imperceptibility. Loo and Kingsbury [38] proposed the first work in this area, and this

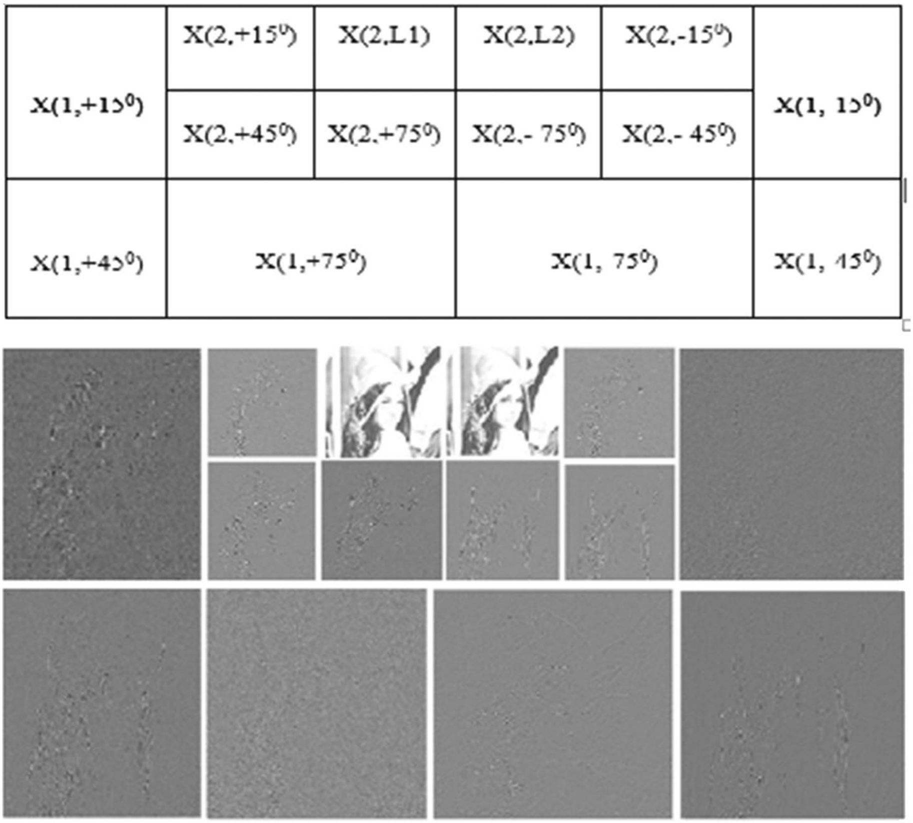


Fig. 3 Two-level DTCWT on *'lena'*

approach has attracted researchers for embedding watermark images [17, 32] and videos [15] in the previous decade.

3.3 Harris corner points

The strong invariance to rotation makes the Harris corner points a popular interest point detector due to their resistance against variation in illumination, scale, rotation, and image noise. This detector depends on the signal's local auto-correlation function; where such functions measure the signal changes locally with the help of patches moved in various directions by a modest amount. In general, the geometrical attack involves changing the positions of pixels in the watermarked images, thus leads to affects its synchronization during the extraction of the watermark. Thus, it's a difficult task to introduce an approach that is robust against all types of geometrical disturbances. One solution to handle this synchronization attack is to find the invariant points which are robust against geometrical attacks for embedding the watermark [20]. Henceforth, to make our proposed approach robust against rotation and translation, the Harris corner feature points of [8] are used. The average optimized Harris points detected in our experiment are 4100 on our standard test images. The three watermark images of size 32*32 of about 3072 bits are embedded into the identified optimized points. Finally, the pseudo-Zernike moments of about 136 moments for 15th order computed from the original cover image are embedded as the fourth watermark. As there is more several identified optimized blocks, these moments can be embedded repeatedly. This helps for better recovery of the tampered region due to unintentional attacks.

Let **I** as an image**.** Let's sweep a window *w(x,y)* on **I** and compute the intensity variation.

$$\mathrm{E}(u,v) = \sum_{x,y} w(x,y)\left[\mathrm{I}(x+u,y+v) - \mathrm{I}(x,y)\right]^2 \tag{12}$$

where,

$w(x,y)$ is the window at position (x,y)

$\mathrm{I}(x,y)$ represents intensity at (x,y)

$\mathrm{I}(x+u,y+v)$ represents moved window position's $(x+u,y+v)$ (intensity)

Since the window with corners is needed, we concentrated on large intensity variation windows. Hence, the above equation has to be maximized as,

$$\sum_{x,y} \left[\mathrm{I}(x+u,y+v) - \mathrm{I}(x,y)\right]^2 \tag{13}$$

Using *Taylor expansion*:

$$\mathrm{E}(u,v) \approx \sum_{x,y} \left[\mathrm{I}(x,y) + u\mathrm{I}_x + v\mathrm{I}_y - \mathrm{I}(x,y)\right]^2 \tag{14}$$

Expanding the equation and cancelling properly:

$$\mathrm{E}(u,v) \approx \sum_{x,y} u^2\mathrm{I}_x^2 + 2uv\mathrm{I}_x\mathrm{I}_y + v^2\mathrm{I}_y^2 \tag{15}$$

It is represented in a matrix as:

$$\mathrm{E}(u, v) \approx [u \;\; v]\left(\sum_{x,y} w(x, y)\begin{bmatrix} \mathrm{I}_x^2 & \mathrm{I}_x\mathrm{I}_y \\ \mathrm{I}_x\mathrm{I}_y & \mathrm{I}_y^2 \end{bmatrix}\right)\begin{bmatrix} u \\ v \end{bmatrix} \tag{16}$$

Let's denote:

$$\mathrm{M} = \sum_{x,y} w(x, y)\begin{bmatrix} \mathrm{I}_x^2 & \mathrm{I}_x\mathrm{I}_y \\ \mathrm{I}_x\mathrm{I}_y & \mathrm{I}_y^2 \end{bmatrix} \tag{17}$$

So, our equation now is:

$$\mathrm{E}(u, v) \approx \begin{bmatrix} u & v \end{bmatrix}\mathrm{M}\begin{bmatrix} u \\ v \end{bmatrix} \tag{18}$$

For each window, a score is calculated, for determining whether the corner is contained,

$$\mathrm{R} = \det(\mathrm{M}) - \mathrm{k}(\mathrm{trace}(\mathrm{M}))^2 \tag{19}$$

where,

det(M)	$\lambda_1\lambda_2$
trace(M)	$\lambda_1 + \lambda_2$

Here, λ_1 and λ_2 are the M's Eigen values. For a window whose **R** score **is** greater than a "corner".

3.4 Cuckoo search optimization

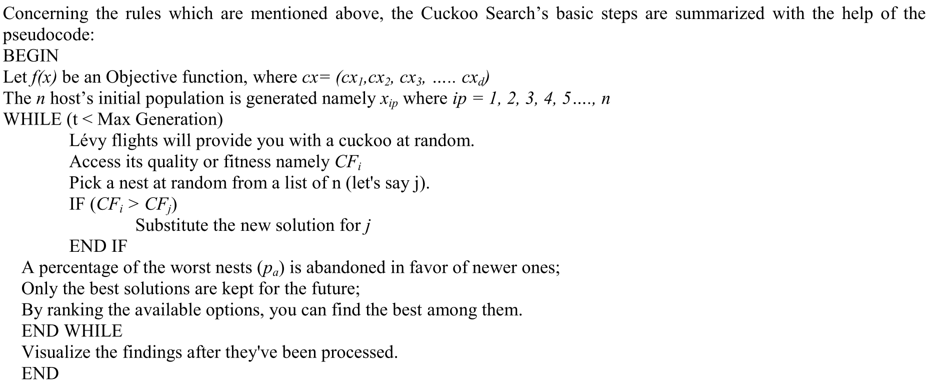
A new metaheuristic approach based on Nature-Inspired Algorithms (NIA) is Cuckoo search Optimization. The cuckoo's breeding behavior was inspired by the modern optimization approach and here it also combines the behavior that can be exposed in some birds and fruit flies namely the Lévy flight. The egg of the cuckoo is considered a solution that is new among the solutions (each egg) on the nest. The main aim is to replace the solutions in the nest which is not that good with cuckoo solutions that are new and potential. To make it simple, let's consider one egg in each nest [61, 62].

The general rules of Cuckoo Search are:

(i) An egg that is laid by cuckoo at a time is dumped into a nest that is randomly chosen.
(ii) Best nests (solutions) with high-quality eggs will be passed down to future generations;
(iii) Here, the host nests number that is accessible is fixed, and the p_a *[0, 1]* is defined as the probability of finding an alien egg by a host. To do so, the host either throws the eggs or abandons the nest, allowing it to create a new nest in a different site.

For ease, the latest statement can be estimated by a fraction p_a of the n number of nests that are being replaced by nests that are new and thus having a new random solution.

The following Levy flight is utilized when the new solution $cx_i(t+1)$ for the i^{th} cuckoo is generated.



Concerning the rules which are mentioned above, the Cuckoo Search's basic steps are summarized with the help of the pseudocode:

```
BEGIN
Let $f(x)$ be an Objective function, where $cx= (cx_1,cx_2, cx_3, ..... cx_d)$
The $n$ host's initial population is generated namely $x_{ip}$ where $ip = 1, 2, 3, 4, 5...., n$
WHILE (t < Max Generation)
        Lévy flights will provide you with a cuckoo at random.
        Access its quality or fitness namely $CF_i$
        Pick a nest at random from a list of n (let's say j).
        IF $(CF_i > CF_j)$
                Substitute the new solution for $j$
        END IF
  A percentage of the worst nests ($p_a$) is abandoned in favor of newer ones;
  Only the best solutions are kept for the future;
  By ranking the available options, you can find the best among them.
  END WHILE
  Visualize the findings after they've been processed.
  END
```

Algorithm 1 The general form of the Cuckoo search algorithm

$$cxi(t+1) = cxi\ (t) + \alpha \oplus Levyflight(\lambda) \tag{20}$$

where α represents step size that is related to the size of the problem of interest. $\bigoplus$ represents multiplications that are based on entry-wise.

4 Proposed system

This section elaborated on the key aspects incorporated into the proposed image watermarking technique which uses meta-heuristic based watermarking in the DTCWT domain. The suggested work's novelty can be summarized as: In this research work, the DTCWT-based coefficients are used for achieving maximum embedding capacity. The Rotation and noise invariance properties of Pseudo Zernike moments make the system attain the highest level of robustness when compared to conventional watermarking systems. To achieve authentication and proof of identity, the watermarks of about four numbers are used for embedding as a replacement for a single watermark image in traditional systems. Among four watermarks, three are the biometric images namely Logo or unique image of the user, fingerprint biometric of the owner, and the metadata of the original media to be transmitted. In addition, to achieve the tamper localization property, the Pseudo Zernike moments of the original cover image are obtained as a feature vector and also embedded as a watermark. To attain a better level of security, each watermark is converted into Zernike moments, Arnold scrambled image, and SHA outputs respectively. In addition, the watermarked image is also signed by the owner's other biometric namely digital signature, and converted into Public key matrix P_{km} and embedded onto the higher frequency subband namely, HL of the 1-level DWT. The better visual quality is achieved by converting the input cover image into the YCbCr form of an image and this $\mathrm{Y_C}$ component is transformed into DTCWT coefficients. After that, optimization using cuckoo search is applied to the resultant DTCWT coefficients which find the suitable embedding position with the parameters of the fitness function such as SSIM (for imperceptibility), Capacity, and Pseudo Zernike moments centered on the high Energy Harris Corner points. Then, calculate SVD on the identified location which is optimal among the DTCWT coefficients, and the singular values which are obtained are further modified with the principal components of the modified multiple watermarks discussed above. The computation of inverse DTCWT results in the watermarked image *WI*. The proposed system also accomplishes a multi-level authentication, among that the first level is attained by the decryption of the extracted multiple watermark images with the help of the appropriate decryption mechanism which is followed by the comparison of the authentication key which is extracted using the key which is regenerated at the receiver's end. The result of authentication is considered a success when the likeness is above threshold value T, authentication is considered successful otherwise, the received watermarked image is considered unauthenticated. In the terms of successful scenarios, the watermark images get extracted and for the unsuccessful cases, the severity of tampering is determined based on unintentional or intentional attacks. The recommended work involves the following stages namely, Embedding, Authentication, Extraction, and Tamper detection and recovery Process.

4.1 Algorithm 2: Embedding process

The novel embedding idea used here involves embedding randomized multiple watermark images on the optimized embedding pseudo-Zernike feature vectors calculated over the Transform coefficients using DTCWT. The embedding process can be elaborated as follows: (i) Pre-processing of cover image, (ii) optimal embedding location, (iii) Multiple watermark images pre-processing, (iv) Process of embedding, and (v) generation of the authentication key. *Pre-processing of Cover Image:* First, convert the RGB color image into *YCbCr* components and apply a two-level DTCWT on Y_C component. From the resultant 16 sub-bands of DTCWT, Harris corner points that are invariant are obtained. *Optimization:* Next, we compute pseudo-Zernike moments for each block of size 15*15 which is centered on the invariant Harris corner feature points. Then, the optimization is accomplished with the help of Cuckoo search's fitness function that varies based on two sets of parameters one based on SSIM, NCC, and payload and the other on PZM which is followed by SVD calculation on the selected coefficients. *Watermark Images Pre-processing:* For authentication and security of the transferred content, multiple watermarks are used and these watermarks are randomized as for watermark 1, the Zernike moments are extracted, for watermark 2 the Arnold scrambling is applied using key K (i.e., 32 for this experiment), for watermark 3, SHA-128 is applied and for watermark 4, the PZM of the cover image is obtained (i.e., order 14 for this experiment). Calculate SVD on these watermarks. *Process of Embedding the Watermarks:* The resultant randomized watermark images are now embedded onto the cover image's singular values. Then the inverse SVD and DTCWT result in a watermarked image. The optimal embedding location increases visual quality, robustness, payload, and security. The process of embedding in the DTCWT coefficients provides more embedding capacity, which in turn promotes its visual perception. The introduction of optimized embedding also improves the robustness and security of the proposed system. *Authentication Key's Generation:* The key used for authentication is formed from the received image and the digital signature, the biometric image of the owner is used to generate the public key matrix which is used to test the authenticity of the watermarked image. The flowchart representation of the meta-heuristic embedding process using the coefficients of DTCWT is shown in Fig. 4. A similar approach is elaborated with the help of the following algorithm.

Input: Cover image 'C_I', Watermark images 'w_i', and owner's biometric image 'B_i'
Output: watermarked image '*WI*' and authentication key 'K_a'

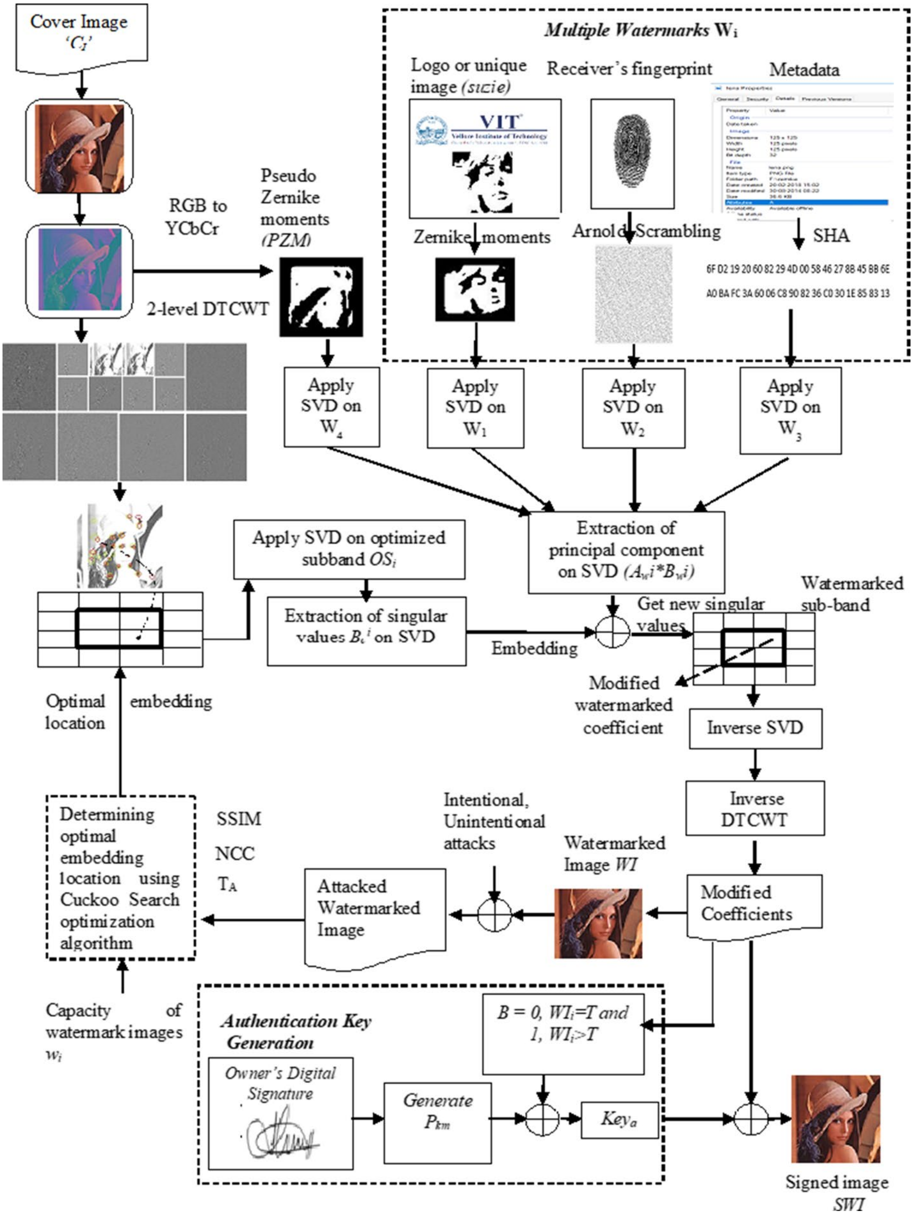

Cover Image
'C_I'
RGB to YCbCr
Pseudo Zernike moments (PZM)
2-level DTCWT
Multiple Watermarks W_i
Logo or unique image (sicie)
Receiver's fingerprint
Metadata
Zernike moments
Arnold Scrambling
SHA
6F D2 19 20 60 82 29 4D 00 58 46 27 8B 45 BB 6E
A0 BA FC 3A 60 06 C8 90 82 36 C0 30 1E 85 83 13
Apply SVD on W_4
Apply SVD on W_1
Apply SVD on W_2
Apply SVD on W_3
Apply SVD on optimized subband OS_i
Extraction of principal component on SVD ($A_{wi}*B_{wi}$)
Extraction of singular values B_t^i on SVD
Embedding
Get new singular values
Watermarked sub-band
Modified watermarked coefficient
Optimal location
embedding
Inverse SVD
Inverse DTCWT
Determining optimal embedding location using Cuckoo Search optimization algorithm
SSIM
NCC
T_A
Intentional, Unintentional attacks
Watermarked Image WI
Attacked Watermarked Image
Modified Coefficients
Capacity of watermark images w_i
Authentication Key Generation
Owner's Digital Signature
Generate P_{km}
$B = 0, WI_i = T$ and $1, WI_i > T$
Key_a
Signed image SWI

Fig. 4 Embedding Process

Step 1. Pre-processing of Cover Image:

(i). Divide the RGB cover image 'C_I' into YCbCr as

$$YC = YCbCr(CI) \tag{21}$$

(ii). Perform DTCWT for two levels on the luminance part Y of the obtained image Y_C

$$\begin{gathered}\left[L_{1R}, L_{1I}, \left[H_{11R}, H_{11I}, H_{12R}, H_{12I}, H_{13R}, H_{13I}, H_{14R}, H_{14I}, H_{15R}, H_{15I}, H_{16R}, H_{16I}\right]\right] = DTCWT\left(Y_C\right) \\ \left[L_{2R}, L_{2I}, \left[H_{21R}, H_{21I}, H_{22R}, H_{22I}, H_{23R}, H_{23I}, H_{24R}, H_{24I}, H_{25R}, H_{25I}, H_{26R}, H_{26I}\right]\right] = DTCWT\left(L_{1R}, L_{1I}\right)\end{gathered} \tag{22}$$

where,

L_1, L_2–2 real and 2 imaginary low frequency subbands of the first and second level.

H_1, H_2, H_3, H_4, H_5, H_6–6 real and imaginary high frequency subbands of the first and second level.

(iii). On each sub-bands of DTCWT coefficients, the feature points which is invariant are obtained using using Harris corner detector,

$$points\left(L_{21}, L_{22}\right) = detectHarrisFeatures\left(L_{21}, L_{22}\right) \tag{23}$$

$$points\left(H_1, H_2, H_3, H_4, H_5, H_6\right)^r = detectHarrisFeatures\left(H_1, H_2, H_3, H_4, H_5, H_6\right)^r \tag{24}$$

where

r = 1,2,3 ……12 direction of sub-bands

(iv). The energy is calculated for the coefficients of DTCWT blocks that are centered on each low-frequency and high-frequency subband point as

$$Energy\ E = \sum\nolimits_{r=1}^{k} \sum\nolimits_{i=1}^{M} \sum\nolimits_{j=1}^{N} \left|X_r(i,j)\right| \tag{25}$$

where,X – points on subbands of low frequency *points($L_{pR,\ pI}$)* and high frequency *points($H_{qR,\ pI}$)^r with p = 1,2 and q = 1,2,….12 directions*

Step 2. Determination of suitable location for embedding using optimization:

(i). The Pseudo Zernike Moments are calculated for the maximum energy invariant blocks and it is considered as an input to the meta-heuristic optimization algorithm.

$$\mathrm{PZM_E} = \mathrm{PZM(E)} \tag{26}$$

(ii). The optimization using the Cuckoo search (discussed in Algorithm 6) is for finding the blocks that are invariant as well as suitable to embed the multi-biometric watermarks.

(iii). The optimization process mainly depends on higher Imperceptibility (SSIM), Embedding Capacity, and PZM$_\mathrm{E}$ which are computed in ***Step 2(i)*** as an objective function.

Step 3. Preprocessing of Multiple Watermark Images:

(i). Watermark 1: The RGB Watermark image which is either logo or unique image 'WU_{img}' is converted into YCbCr component and finds its Zernike Moments as,

$$\begin{aligned}&Y_{w1}Cb_{w1}Cr_{w1} = YCbCr\left(WU_{img}\right) \\ &w1 = PZM(Yw1)\end{aligned} \tag{27}$$

(ii). Watermark 2: To verify the authentication of the content, the expected receivers' fingerprint 'WF_b' of size M*N are randomized using Arnold transformation with

Key *K,* and from that encrypted fingerprints generate a matrix of size P*Q using Bi-directional Associative Memory Networks as given in [48] where P – number of receivers and Q – M*N and encrypt the with pseudorandom number *Kp* as

$$R_b = E_K\left(WF_b\right) \tag{28}$$

where,*b* = *1,2, 3……..Q number of receivers*

$$w_2 = E_{Kp}(BAM(Rb, P)) \tag{29}$$

(iii). Watermark 3: The cover image *Mc*'s metadata is considered as 3rd watermark image and which is encrypted using Secure Hash Algorithm SHA to provide a level of security.

$$w_3 = SHA(Mc) \tag{30}$$

(iv). Watermark 4: The PZM of the input cover image is calculated and used for tamper detection and recovery,

$$w_4 = PZM\left(Y_C\right) \tag{31}$$

Step 4. Embedding of Multiple Watermarks:

(i). Calculate SVD on each PZM invariant point *(OPZM$_E$)* of the optimized and embeddable cover image generated by Algorithm 6, and it is given as,

$$\left[A_c^{pt}, B_c^{pt}, C_c^{pt}\right] = SVD\left(OPZM_E\right) \tag{32}$$

where,

B_c^{pt} represents the singular values of *t* number of matrix points *p.*
A_c^{pt} and C_c^{pt} represent *p* matrix points and *t* orthogonal matrices.

(ii). Similarly, compute SVD on each multi-biometric watermark image i which is obtained as a result of Step 3 as,

$$\left[A_w^i, B_w^i, C_w^i\right] = SVD\left(w_i\right) \tag{33}$$

where, i = 1, 2, 3, 4 number of watermarks

(iii). Calculate the modified singular values of points *t* as $B_c^{pt'}$, by simply combining the cover image singular value B_c^{pt} with the principal component ($A_w^{\,i} \times B_w^{\,i}$) of the watermark image whose significance is determined by multiplying with the scaling factor α.

$$B_c^{pt'} = B_c^{pt} + \alpha \left(A_w^i \times B_w^i\right) \tag{34}$$

where, α represents robustness factor.

(iv). Inverse SVD is performed to obtain the modified coefficients of the optimized blocks as:

$$A^{pt'} = A_c^{pt} \times B_c^{pt'} \times C_c^{pt} \tag{35}$$

(v). The watermarked image namely qcf$_1$' is thus obtained using the inverse DTCWT as,

$$\begin{aligned}(L_{1R}', L_{1I}') &= IDTCWT[[L_{2R}', L_{2I}', [H_{21R}', H_{21I}', H_{22R}', H_{22I}', H_{23R}', H_{23I}', H_{24R}', H_{24I}', H_{25R}', H_{25I}', H_{26R}', H_{26I}']]] \\ Y_C' &= IDTCWT\Big[[L_{1R}', L_{1I}', [H_{11R}, H_{11I}, H_{12R}, H_{12I}, H_{13R}, H_{13I}, H_{14R}, H_{14I}, H_{15R}, H_{15I}, H_{16R}, H_{16I}]]\end{aligned} \tag{36}$$

(vi). The resultant *Yc'* in (vi) is converted to a normal RGB image resulting in the watermarked image *'WI'.*

Step 5. Generation of Authentication key and Embedding:

To provide additional authentication at the receiver side, the key Key_a is generated as an authentication key, that is used for checking the legitimacy of the received watermarked image before extraction. To do so, the owner's digital signature biometric and the uncorrupted watermarked image which is the original *WI* are used to generate the public key P_{km}. The key generation process is elaborated as,

(i). Apply adaptive thresholding on watermarked image *WI*, so that binary image is obtained as

$$\begin{matrix} B = 0, WI_i <= T\ and \\ 1, WI_i > T \end{matrix} \tag{37}$$

(ii). Compute the authentication key $\mathrm{Key_a}$ as

$$Key_a = XOR(P_{km}, B) \tag{38}$$

(iii). The authentication key once generated is embedded onto the HL subband of two-level DWT of the watermarked image *WI* and it is described below,

a. The DWT is performed mainly to acquire the subbands which are multiresolution.
b. The PCA is computed on the HL subband to obtain the uncorrelated coefficients on the subband as $\mathrm{HL_p}$
c. The above obtained uncorrelated PCA coefficients are modified as

$$\mathrm{HL_p}' = \mathrm{HL_p} + \alpha \times \mathrm{Key_a} \tag{39}$$

where for this experiment the robustness factor α is considered as 0.6

4. The Inverse PCA is performed.

(iv). Thus, the watermarked image which is of signed form *SWI* is obtained.

4.2 Algorithm 3: Watermark Detector and the process of Extraction

The watermark detector and process of extraction involve the reverse of the embedding process. It includes the following stages (i) the first level of authentication of watermarked image, (ii) Multi-biometric Watermarks Detection, (iii) Extraction of Multi-biometric Watermarks, and (iv) Next level of authentication - Tamper detection and Recovery and Tamper detection and Fragile. *The first level of Authentication:* To check whether the watermarked image which is received is authenticated or not, the key $\mathrm{K_a}''$ is computed from a received image using the same process as in embedding and it is compared with key K_a' (extracted from HL band of 2-level DWT). If both match, then there is "No change" in the received content else, the received content has been tampered with. Thus, the first level of authentication is proved. *Detection:* The watermark's presence is verified by computing the normalized correlation coefficient between the received image (which might be corrupted) and the cover image. Then this correlation result is compared with the predefined threshold. Hence, if the value of correlation is higher than a defined threshold, then a 'watermark' is available, else, there is 'no watermark'. *Extraction:* During extraction, the second level of authentication is performed and it leads to the following cases (i) when the authentication succeeds, the tampered region is detected and the recovery has happened as it is due to unintentional attacks, and (ii) when the authentication does not succeed the tampered region is detected and fragile as the tampering is due to intentional attacks. For the mentioned cases of the authentication process, we start extracting the watermark image and the comparison of pseudo-Zernike moments of received watermarked image with extracted watermark 4 happens after watermark post-processing. *Watermark post-processing:* From the extracted multi-biometric watermarks namely (i) watermark 1, extracted Zernike moments are reconstructed to get the original image unique image or logo, (ii) watermark 2, scrambled fingerprint image of the receiver can be extracted using the appropriate (Arnold) key by an authorized user and it can also be compared with the receiver's fingerprint to validate the second level of authentication, (iii) watermark 3, metadata of the cover image is also used to validate the authenticity of the content and it leads to the third level of authentication, and watermark 4, extracted Pseudo Zernike moments of the original cover image is used as a feature vector not only for the detecting the region of tampering but also for recovering it. The detailed flowchart representing the extraction process is given in Fig. 5 and the same is elaborated below:

Input: Unique owner's biometric image *'B_i'*, Signed watermarked image *'SWI'* (might be corrupted)

Output: multi-biometric watermark images w_i*', the* decision on tamper detection

Step 1. Watermarked Image Authentication (first – level):

(i). Apply adaptive thresholding on the received signed watermarked image *'SWI'* similar to the one performed at the embedding (Step 5 - i) to extract the binary image as,

$$\begin{aligned} &B_i^{\}} = 0, WI_i^{'} <= T \; and \\ &Bi^{\}} = 1, WI_i^{'} > T, for \; i = 1, 2, 3, \ldots .m \end{aligned} \tag{40}$$

(ii). Calculate an authentication key $\mathrm{Key^a{}_i}$' as

$$Key^a{}_i^{'} = XOR\left(P_{kmi}{}^{'}, B_i^{'}\right) \text{ refers embedding process for the generation of } P_{kmi}{}^{'}$$
$$Key_a^{''} = Average\left(Key^a{}_i^{'}\right), for \; i = 1, 2, 3, \ldots .m \tag{41}$$

(iii). On received watermarked image,

a. Apply DWT for obtaining the multiresolution subbands.
b. To find the uncorrelated coefficients, the PCA is calculated on the HL subband as $\mathrm{HL_p}$"
c. Then, from those PCA coefficients, the key which is used for authentication is extracted as

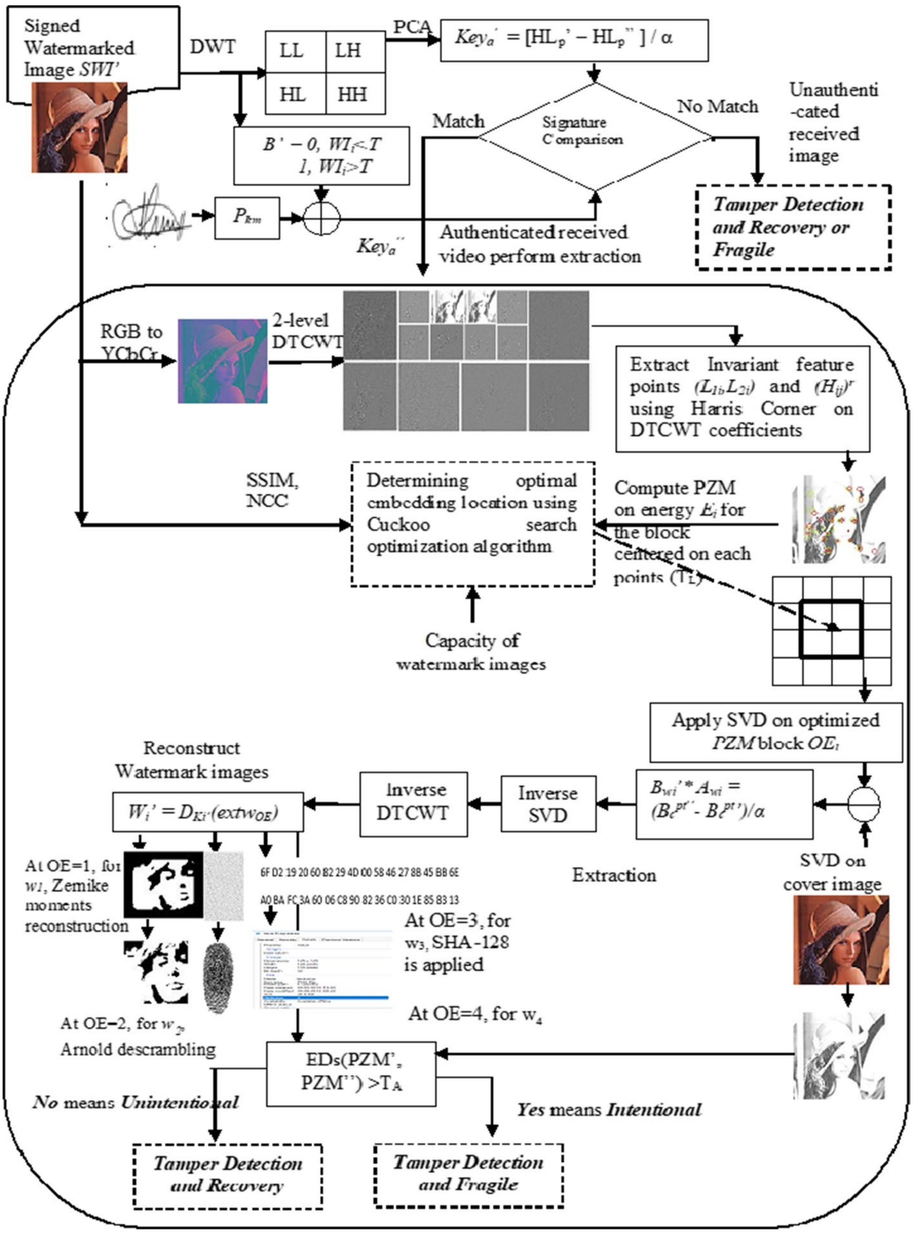

Signed Watermarked Image SWI'
DWT
LL
LH
HL
HH
PCA
Key_a' = [HL_p' – HL_p''] / α
B' – 0, WI_i<T
1, WI_i>T
P_Rm
Key_a''
Match
Signature Comparison
No Match
Unauthenti-cated received image
Tamper Detection and Recovery or Fragile
Authenticated received video perform extraction
RGB to YCbCr
2-level DTCWT
Extract Invariant feature points (L_1i,L_2i) and (H_ij)^r using Harris Corner on DTCWT coefficients
SSIM, NCC
Determining optimal embedding location using Cuckoo search optimization algorithm
Compute PZM on energy E_i for the block centered on each points (T_i)
Capacity of watermark images
Apply SVD on optimized PZM block OE_i
Reconstruct Watermark images
W_i' = D_Ki'(extw_OE)
Inverse DTCWT
Inverse SVD
B_wi'* A_wi = (B_c^pt'' - B_c^pt')/α
SVD on cover image
Extraction
At OE=1, for w1, Zernike moments reconstruction
6F D2 19 20 60 82 29 4D 00 58 46 27 8B 45 BB 6E
A0 BA FC 3A 60 06 C8 90 82 36 C0 30 1E 85 83 13
At OE=3, for w3, SHA-128 is applied
At OE=2, for w2, Arnold descrambling
At OE=4, for w4
EDs(PZM', PZM'') >T_A
No means Unintentional
Yes means Intentional
Tamper Detection and Recovery
Tamper Detection and Fragile

Fig. 5 Extraction Process

$$\mathrm{Key_a}{}' = \left(\mathrm{HL}_p^{i\,\prime} - \mathrm{HL}_p^{i\,\prime\prime}\right)/\alpha \tag{42}$$

where α is the factor for robustness

(iv). C = Equate

$$\left(Key'_a, Key''_a\right) \tag{43}$$

```
If $C == true$,
Received content is authenticated
Do
The Process of Extraction (Step 2)
else,
Received content is unauthenticated
Do
If EDs(PZM',PZM") < $T_A$ then
"Unauthentication happens due to Unintentional attacks"
Do
Tamper Detection and Recovery (Algorithm 4)
Else
"Unauthentication due to Intentional attacks"
Do
Tamper Detection and fragile (Algorithm 5)
End If
End If
```

Step 2. Extraction and the post-processing of Multi-biometric Watermarks:

(i). For the received watermarked image, apply DTCWT as in the embedding process Step 1 (iii).

(ii). The Harris corner detector is used to extract an invariant feature point similar to an embedding process Step 1 (iv).

(iii). Calculate energy and Pseudo Zernike Moments for coefficients of DTCWT which is focused on every Harris point as in Step 1(v) for obtaining the PZM from the maximum energy block.

(iv). Then, to obtain the location which is suitable for embedding OE_f, the PZM, and energy calculated in step (iii) are provided as an input to *Algorithm 6*.

(v). Assume that each optimized PZM invariant point OE_f' has SVD applied to it and given as

$$\left[A_c^{pt'}, B_c^{pt''}, C_c^{pt'}\right] = SVD\left(OE'\right)pt \tag{44}$$

where,

$B_c^{pt''}$ *a*singular values of *p* matrix points *for t* number.
$A_c^{pt'}$ and $C_c^{pt'}$ – orthogonal matrices of *p* matrix points *for t* number.

(vi). The multi-biometric watermarks principal component is extracted by the equation as,

$$B_w{}' * A_w = \left(B_c^{pt''} - B_c^{pt'}\right)/\alpha \tag{45}$$

(vii). Over the principal component, B_w'* A_w which is extracted apply inverse SVD to obtain each watermark image i,

$$Extw_i = A_w{}^i \times B_w{}^{i'} \times \left(C_w{}^i\right)^T \tag{46}$$

(viii). Apply Inverse DTCWT which results in a randomized form of each watermark image.

(ix). Apply Zernike moments reconstruction on *Extw$_1$*, Arnold Key *K′* on *Extw$_2$, and* SHA-128 on *Extw$_3$* to get the original form of watermarks

$$DS^i = D_{K'}\left(extw_i\right)\ (second\ level\ of\ authentication) \tag{47}$$

(x). Repeat the above five steps from (vi) to (x) of this extraction process aimed at various values of *i* = *1 to 4* to get the multiple watermarks *w$_i$'*, where we normally consider the watermark image length equal to half of the length of cover image *m*.

4.3 Algorithm 4: Tamper detection and recovery

To deal with the authentication of data over insecure online social networks, the robust and semi-fragile form of a watermark detector is introduced in our proposed approach. The proposed approach deals with the term semi-fragile because the attacks that happened during communication can be both intentional and unintentional, where the invariant optimized feature points are resilient to unintentional attacks, whereas intended attacks are vulnerable. The attacks namely noise addition, geometrical variation, and JPEG compression are normally treated as unintentional because these variations won't change the complete image or its meaning. Therefore, such alterations or tampers need to be detected and recovered (leads to Tamper detection and recovery). On the other hand, the attacks such as cropping, replacing, copy-move, and image splicing are considered intentional and will have severe implications. Hence, such attacks need to be detected but not recovered instead it has to be collapsed to avoid conveying wrong information from such images (leads to Tamper detection and fragile).

During this stage, the received watermarked image *WI'*, is considered unauthentic thus, when the first level of authentication fails. This process of authentication is carried out by setting a threshold T_A *(i.e 3120 in our experiment)* to classify the image which is received either as intentional or unintentional. It is deliberated by computing squared Euclidean distance *EDs* among the extracted pseudo-Zernike moments *PZM*' and the one which is computed from the corrupted image *PZM"*. The absolute form of squared Euclidean distance is used because certain variations are shown deeper and there won't be any compromise between the rate of recognition and robustness to alterations.

The pseudo-Zernike moments are generated as per Eq. (8) centered on the Harris corner points over the DTCWT coefficients. Also, extract the watermarks from the optimized location identified using Algorithm 6. Then, compare the extracted pseudo-Zernike moments PZM' (watermark 4) with the computed PZM". The distance between the two different feature vectors is calculated using the squared Euclidean distance. To decide on the distances the threshold $\mathrm{T_A}$ is used and it is obtained from the meta-heuristic optimization algorithm (Algorithm 6) were calculated by defining an objective function based on average over a minimum of false positive and false negative probability on Receiver operating characteristics and a minimum of squared Euclidean distance obtained by performing various manipulations on the watermarked image. The false-negative and positive probability for various threshold limits from 2500 to 5000 are depicted in the Table 2

Table 2 False Negative and Positive Probabilities for various Threshold Limits

Threshold	False Positive probability	False Negative probability
2500	0.0235	0.0014
2600	0.0234	0.0022
2700	0.0232	0.0036
2800	0.0230	0.0045
2900	0.0222	0.0046
3000	0.0217	0.0047
3100	0.0215	0.0051
3200	0.0216	0.0055
3300	0.0210	0.0057
3400	0.0208	0.0059
3500	0.0207	0.0061
3600	0.0206	0.0062
3700	0.0205	0.0064
3800	0.0204	0.0066
3900	0.0203	0.0067
4000	0.0201	0.0075
4500	0.0200	0.0083
5000	0.0197	0.0100

$$Attacks = \begin{cases} Unintentional\ Attacks\ (Sec.VD2\ ), EDs\left(PZM', PZM''\right) < T_A \\ Intentional\ Attacks(Sec.VD3\ ), EDs\left(PZM', PZM''\right) \geq T_A \end{cases} \\ (Third\ level\ of\ authentication) \tag{48}$$

where *PZM'* and *PZM"* are the pseudo-Zernike feature vectors of the images f1(x,y) = C_I original cover image and f2(x,y) = *WI*. The PZM_i' = (PZM*i*,1,PZM*i*,2,. ..,PZM*i*,*N*) = ($PZ_{15,0,}$ $PZ_{15,1,}$ $PZ_{15,2,}$ $PZ_{15,3,}$ $PZ_{15,4,}$ $PZ_{15,5,}$ $PZ_{15,6,}$ $PZ_{15,7,}$ $PZ_{15,8,}$ $PZ_{15,9,}$ $PZ_{15,10,}$ $PZ_{15,11,}$ $PZ_{15,12,}$ $PZ_{15,13,}$ $PZ_{15,14,}$ $PZ_{15,15}$ for order 15 from Table 2. When the different attacks happened on the watermarked image i.e., the feature vectors $f1(x, y)$ and we get $f2(x, y)$ and its distance are calculated.

From the above distance equation, it is clear that tamper detection and recovery will be performed for the identified unintentional attacks such that $EDs < T_A$. Whereas, tamper detection and fragile happen when it is identified as intentional attacks.

4.3.1 Tamper detection and recovery

To detect the location of the tamper and to proceed with the recovery, the following activities are done. First, we used the rotation and translation invariant properties of the Harris corner detector by computing its feature points on the DTCWT coefficients of the original image. The pseudo-Zernike feature points are computed centered on these maximum energy Harris feature points of size 15*15 (in our experiment). This utilizes the noise and rotation invariant property of pseudo-Zernike moments. Secondly, to use it better, the pseudo-Zernike moments of about 136 obtained from 15th order on the original image are also embedded onto these pseudo-Zernike feature points obtained from the Harris corner feature points. Thus, the tampered regions are perfectly located on the watermarked image by simply comparing the extracted pseudo-Zernike moments PZM' of an ith block from the regenerated moments on the received watermarked image PZM" of the same ith block with the threshold T$_B$ (i.e 512 in our experiment). The region of moments that do not match helps us to locate the region of tampering.

$$Tampered\ region = \begin{cases} Attacked\ region, & \left|PZM'^{i} - PZM''^{i}\right| > T_B \\ Unattacked\ region,, & \left|PZM'^{i} - PZM''^{i}\right| \leq T_B \end{cases} \tag{49}$$

4.3.2 Recovery

The reconstruction ability of pseudo Zernike moments helps to reconstruct the region which is detected as tampered if it is due to the unintentional attacks.

4.4 Algorithm 5: Tamper detection and fragile

On the other hand, once the received image fails the first level of authenticity and is treated as intentional attacks using Eq. 48, there is a need to decide on the restoration of the tampered area or not. The area which is tampered is considered as sensitive if it is greater than the threshold T$_C$ then instead of tamper recovery, fragile happens otherwise tamper recovery will proceed.

4.5 Algorithm 6 Metaheuristic-based embedding location selection using Cuckoo Search (CS) OE$_f$

Step 1. Initialization

(i). The CS parameters are initialized as nest number (n) = 50, size of nest (s) = 5*watermarks' size, minimum generations in number as t = 0, step size α = 0.25, number of maximum generations in number as G$_{max}$ = 1200

(ii). The Fitness or objective (FO$_n$) is chosen to maximize the visual quality (SSIM), robustness (NCC), and Capacity as,

$$F_1 = \text{Max}\left(\frac{1}{N}\sum_{A=1}^{N} SSIM\left(CI, WI_A\right) + \lambda\ Capacity + \beta\ NCC\right)$$
$$F_2 = T_A = Average\left(\min\left(FP^N_{P,T}, FN^N_{P,T}\right), \min\left(ED_s\left(PZM'_{O,N}, PZM''_{O,N}\right)\right)\right)\ F_n = \text{Max}\left(F_1, F_2\right) \tag{50}$$

where,

C_I	Cover Image,
WI_A	tampered watermarked image
N	total attacks
Adjustment	factors as λ and β for adjusting SSIM, Capacity, and Robustness
SSIM	is assigned the value between 0.9 and 1.0
Capacity	is considered as w_i the multiple watermarks

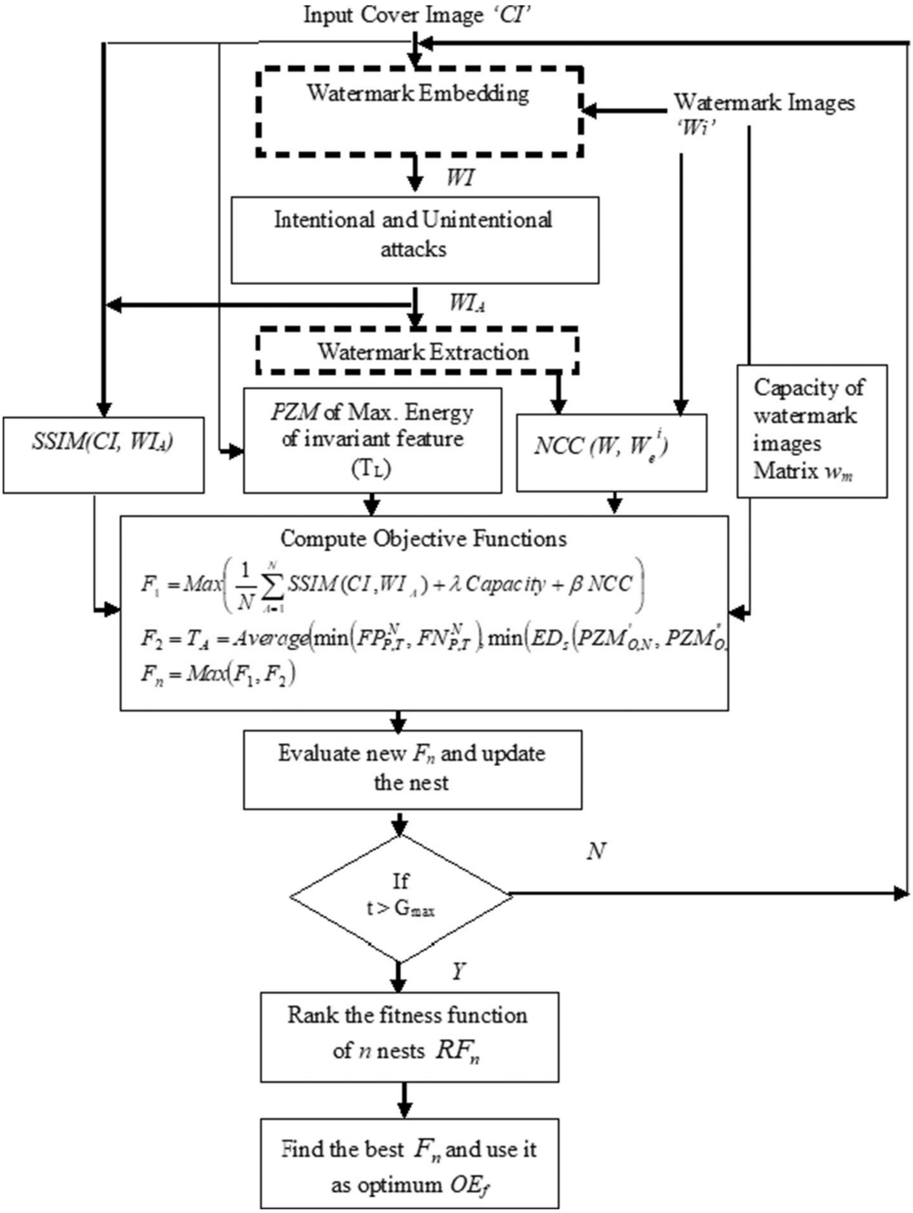

Input Cover Image 'CI'
Watermark Embedding
Watermark Images 'Wi'
WI
Intentional and Unintentional attacks
WI_A
Watermark Extraction
SSIM(CI, WI_A)
PZM of Max. Energy of invariant feature (T_L)
NCC (W, W_e^i)
Capacity of watermark images Matrix w_m
Compute Objective Functions
F_1 = Max(1/N ∑_{A=1}^{N} SSIM(CI, WI_A) + λ Capacity + β NCC)
F_2 = T_A = Average(min(FP_{P,T}^N, FN_{P,T}^N), min(ED_s(PZM'_{O,N}, PZM'_O
F_n = Max(F_1, F_2)
Evaluate new F_n and update the nest
If t > G_max
N
Y
Rank the fitness function of n nests RF_n
Find the best F_n and use it as optimum OE_f

Fig. 6 Metaheuristic algorithm to find the optimal embedding location

T_A Authentication threshold
FP_P *False positive probability*
FN_P *False-negative probability*
EDs is the squared Euclidean distance computed between Pseudo Zernike moments of the original cover image and attacked image of *Oth* order and *N* attacks.

Step 2. Output: The location which is suitable for watermark image embedding is determined using the F_n as in Eq. (50) as is shown in Fig. 6.

Step 3. Selection Process:

(i). WHILE $t < G_{max}$

a. Levy Flights gives a cuckoo at random by *i*.
b. Calculate FO_i using Eq. (50)
c. From the random nests *n*, select a *j* nest and calculate its function FO_j
d. IF $FO_i < FO_j$
e. Substitute *j* with the new solution.
f. ELSE

i. Consider the solution be *i* and
ii. The poorest nest gets abandoned and the nest which is new are built using Levy flights.
iii. Keep the best current one
iv. The numerous *n* nests F_n is ranked to get $R(F_n)$
v. The best F_n is identified and it is used as optimal embedding location OE_f

5 Experimental analysis

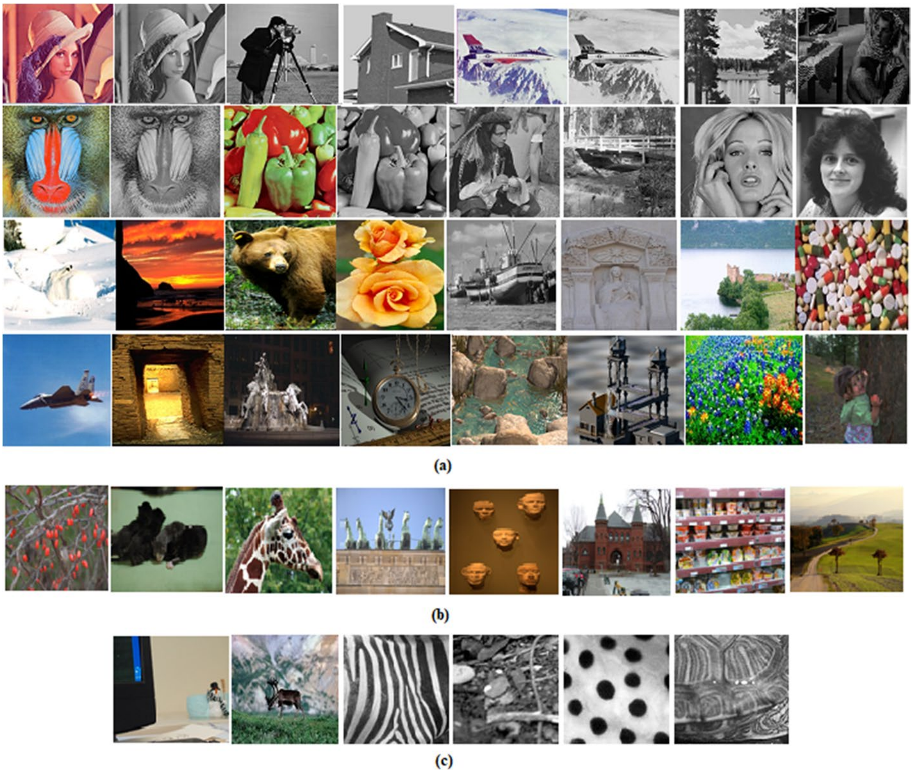
The proposed semi-fragile multi-biometric based content authentication system is validated with the help of various watermarking characteristics namely visual perception, security, payload, and robustness. This section deals with datasets description, quality measures, experimental setup, and results and discussions.

5.1 Datasets Description

The data on online social networks are vulnerable to both intentional and unintentional attacks. The specific datasets have been used to verify the robustness against unintentional and intentional cases. The former case involves attacks namely, image processing operations, geometric distortions, JPEG compression, and Multiple JPEG which can be tested using the standard test image dataset. On the other hand, the latter case involves attacks namely copy-move forgery, image splicing, collage, and cropping which can be tested using MICC, CISDE, and standard test image datasets respectively. To make the forgery image Adobe Photoshop is used.

5.1.1 Standard test images

The standard images which are often used in the literature are *lena, peppers, cameraman, lake,* etc. The standard images are normally in uncompressed *'tif'* format which comprises the images with bright colors, dark colors, textures, smooth areas, lines, and edges are all of the same size 512 × 512 is used as shown in Fig. 7a



(a)

(b)

(c)

Fig. 7 Cover Images (**a**) standard test images (**b**) *MICC – F600 c) CISDE*

5.1.2 MICC – F600

This dataset is a collection of original images of about 440, 160 tampered images, and 160 ground truth images for testing the copy-move forgery detection [14] (see Fig. 7b)

5.1.3 CSIDE

Image splicing also known as copying and pasting is the most common tampering seen today. Columbia Image Splicing Detection Evaluation Dataset (CISDE) provides a benchmark set with only the splicing operation these images are in high resolution and uncompressed. This dataset is not restricted to splicing detection but is also suitable for other computer vision algorithms since the ground truth of exposure settings is accessible [26] (see Fig. 7c)

5.1.4 Fingerprint dataset

The fingerprints of various sets of receivers are captured at various angles and recorded for the experiments. The device used for capturing is MFS100 which merely depends on the optical sensing technology that proficiently identifies even the fingerprints that are of poor

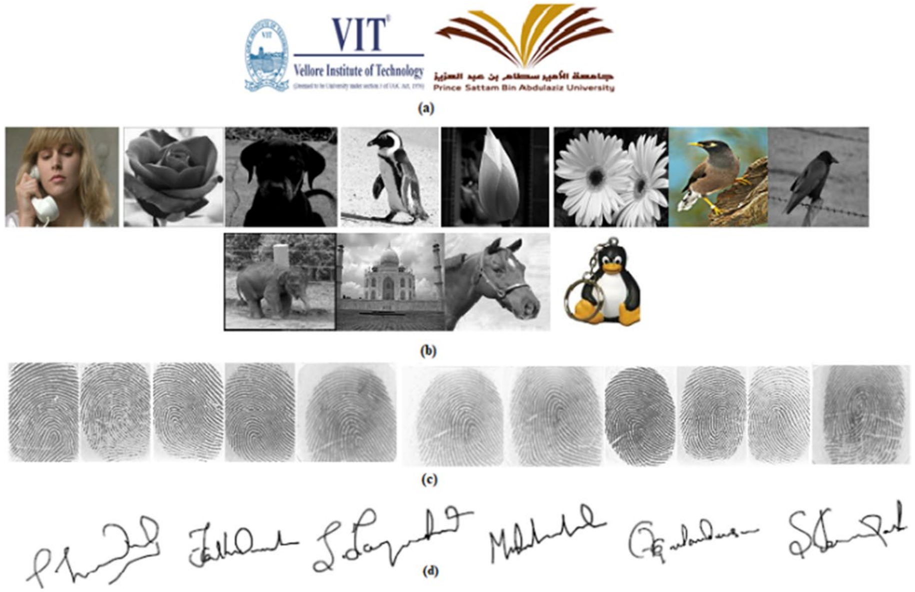

VIT
Vellore Institute of Technology
Prince Sattam Bin Abdulaziz University
(a)
(b)
(c)
(d)

Fig. 8 Watermark Images (**a**) Logo (**b**) unique images (**c**) Receiver's Fingerprints (**d**) Owner's Digital Signature

quality. This MFS100 is mostly designed for identification, and verification and also for the authentication of the owner when their fingerprints are acts like a digital password. It comprises about 100 images uncompressed images of size 32*32 (see Fig. 8c).

5.1.5 Digital signature

The digital signatures of the owners are created using the WACOM One Graphic Tablet. It comprises about 100 images uncompressed images of size 128*32. (see Fig. 8d)

The cover images from the datasets' standard test images, MICC – F600, CSIDE are converted to the same dimensions, and the watermark images namely logo or unique images, receiver's fingerprints, and owner's digital signatures of size smaller than the cover images are considered here for evaluation. The sample cover images of each dataset are shown in Fig. 7 and the watermark images namely logo, unique image, receivers fingerprint, and digital signature are presented in Fig. 8. test images from each dataset and its description are given in Table 3 below.

5.2 Experimental setup

The experiments were carried out with a Windows 10 Professional (64-bit) environment of Lenovo Thinkpad P15v with Intel Core i7 FHD IPS Workstation in a single NVIDIA Quadro P620 4GB Graphics @ 2.60GHz processor speed and 32GB capacity of RAM. For storage purposes, we used a 1 TB Seagate Hard disk drive. The software used for simulation purposes is MATLAB R2019a.

Quality Metrics

Table 3 Details of cover images and watermark images

	Image	Color	Size in *pixels*	Format
Cover Images				
Standard test images	*Lena*	color, gray	512×512	TIF
	Cameraman	gray	512×512	TIF
	House	gray	512×512	TIF
	jetplane	gray	512×512	TIF
	Lake	gray	512×512	TIF
	barbara	gray	512×512	TIF
	baboon	color, gray	512×512	TIF
	peppers	color, gray	512×512	TIF
	pirate	gray	512×512	TIF
	walkbridge	gray	512×512	TIF
	woman_blonde	gray	512×512	TIF
	woman_darkhair	gray	512×512	TIF
	arctic_hare	color	512×512	TIF
	Bandon	color	512×512	TIF
	Bear	color	512×512	TIF
	Brandyrose	color	512×512	TIF
	Fishing boat	Gray	512×512	TIF
	Fourviere	Gray	512×512	TIF
	Lochness	color	512×512	TIF
	opera	color	512×512	TIF
	pills	color	512×512	TIF
	plane	color	512×512	TIF
	Pueblo_bonito	color	512×512	TIF
	terraux	color	512×512	TIF
	watch	color	512×512	TIF
	water	color	512×512	TIF
	waterfalls	color	512×512	TIF
	wildflowers	color	512×512	TIF
	baby	color	512×512	TIF
Standard test images	*Berries*	color	512×512	TIF
	Four_babies	color	512×512	TIF
	Giraffe	color	512×512	TIF
	Horses	color	512×512	TIF
	Mask	color	512×512	TIF
	Redtower	color	512×512	TIF
	Supermarket	color	512×512	TIF
	Tree	color	512×512	TIF
	Table	color	512×512	TIF
	Deer	color	512×512	TIF
	Stripes	gray	512×512	TIF
	Land	gray	512×512	TIF
	Dots	gray	512×512	TIF
	curves	gray	512×512	TIF

Table 3 (continued)

	Image	Color	Size in *pixels*	Format
Watermark Images				
logo	*VIT*	color	128×256	TIF
	PSAU	color	128×256	TIF
Unique images	*Suzie*	color	256×256	TIF
	Rose	gray	256×256	TIF
	Dog	gray	256×256	TIF
	Penguin	gray	256×256	TIF
	Lotus	gray	256×256	TIF
	Flower	gray	256×256	TIF
	Myna	color	256×256	TIF
	Crow	gray	256×256	TIF
	Babyelephant	gray	256×256	TIF
	Tajmahal	gray	256×256	TIF
	Horse	gray	256×256	TIF
	Keychain	color	256×256	TIF
Fingerprint samples	*FP1*	gray	128*64	TIF
	FP2	gray	128*64	TIF
	FP3	gray	128*64	TIF
	FP4	gray	128*64	TIF
	FP5	gray	128*64	TIF
	FP6	gray	128*64	TIF
	FP7	gray	128*64	TIF
	FP8	gray	128*64	TIF
	FP9	gray	128*64	TIF
	FP10	gray	128*64	TIF
	FP11	gray	128*64	TIF
Digital Signatures	*DS1*	gray	32*128	TIF
	DS2	gray	32*128	TIF
	DS3	gray	32*128	TIF
	DS4	gray	32*128	TIF
	DS5	gray	32*128	TIF
	DS6	gray	32*128	TIF

The proposed multi-biometric semi-fragile based watermarking algorithm is developed to protect the multimedia data on online social networks in terms of authentication, visual quality, capacity, and robustness. The metrics generally for measuring visual perception are both the objective one SSIM meant for Structural Similarity Index Measure and the subjective one PSNR meant for Peak Signal-to-Noise Ratio. In addition, to measure the robustness, the metrics used are mostly BER and NCC abbreviated as Bit Error Rate and Normalized Correlation Coefficient respectively. Also a metric for measuring the capacity is introduced in this approach which dealt with the maximum number of multi-biometric watermark images that can be allowed to embed over the cover image. Finally, the authentication is measured at various levels and the corresponding decision is made based on the intentional and unintentional attacks.

5.2.1 Visual perception or imperceptibility

The SSIM and PSNR are the most important metric used for measuring the humiliation caused by the attacks which happen during communication over an insecure network. The minimum acceptable limit of PSNR is above 38 dB [37] and on the other hand, the acceptable limit of SSIM varies from 0 (Zero matches) to 1 (perfect match).

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{51}$$

where Mean Square Error (MSE) between the cover image C_I and attacked watermarked image WI_A is defined as,

$$MSE = \frac{1}{T}\left(\sum_{t=1}^{T}\left(C_I - WI_A\right)^2\right) \tag{52}$$

where T represents a total number of pixels in each image.

The SSIM between two images namely cover image C_I and the attacked watermarked image WI_A is given as,

$$SSIM(x,y) = \frac{\left(2L_{C_I}L_{WI_A}\right)\left(2V_{CI_{WI_A}}\right)}{\left(L^2_{C_I} + L^2_{WI_A}\right)\left(V^2_{C_I} + V^2_{WI_A}\right)} \tag{53}$$

where,

L_{Ci} and L_{Wa} denote the factor of luminance between two given images i.e., the mean of C_I and WI_A

V_{Ci} and V_{WIa} denote the factor of contrast between two given images i.e., the standard deviation of C_I and WI_A

$V_{\mathrm{Ci}}\, V_{WIa}$ denotes the normalized correlation coefficient between C_I and WI_A.

5.2.2 Robustness

The embedded watermark's robustness might be affected by various unintentional and intentional attacks and it can be measured by using NCC and BER. The acceptable limit of all these metrics should range from 0 to 1.

(i). NCC: This metric is computed among the original and extracted watermark to identify its correlation, if its value is close to 1 then those two images are assumed to be correlated otherwise, it is considered to be uncorrelated. This can be calculated with the help of the equation and it is expressed as,

$$NCC = \frac{\sum\left(\left(OW_{k,i} - OW_{i,m}\right)\left(EW_{k,i} - EW_{i,m}\right)\right)}{\sqrt{\sum\left(OW_{k,i} - OW_{i,m}\right)^2}\sqrt{\sum\left(EW_{k,i} - EW_{i,m}\right)^2}} \tag{54}$$

where, $OW_{k,i}$ represents the ith position of original watermark and its kth pixel intensity, similarly, $EW_{k,i}$ represents the ith position of extracted watermark and its kth pixel intensity,

$OW_{i,m}$ represents ith position of original watermark and its mean intensity, and $EW_{i,m}$ represents mean intensity of ith position of extracted watermark.

(ii) BER: The proportion of extracted bits of the watermark which is wrong to the total embedded watermark bits. When there is no error in the message received, then the value of the bit error rate will be 0, else, it will be closer to 1.

It is represented as follows,

$$BER\left(OW_i, EW_i\right) = \frac{\sum_{i=1}^{m} \mid OW_{k,i} - EW_{k,i} \mid}{m} \tag{55}$$

where, $OW_{k,i}$ is the intensity of the kth pixel in an ith original watermark, $EW_{k,i}$ is the intensity of the kth pixel in an ith extracted watermark, and m is the total number of embedded watermark bits which is obtained as $m_1 + m_2 + m_3 + m_4$.

5.2.3 Payload

In general, the payload of the watermark dealt with the maximum number of coefficients obtained due to the transform being suitable for watermark embedding, to be precise it should not only degrade the visual perception but also the robustness of the watermarking system. Here, DTCWT provides more transform coefficients and it is most suitable for embedding the watermark. To achieve the maximum capacity as in [3], we also used Pseudo Zernike Moments. It is expressed as, for an order of 15, we can have 136 moments and from these 130 can be used. Hence, for the given image size of 512×512, approximately 230,000 bits are suitable to embed without the degradation of mere visual perception as well as robustness level. Therefore, the most desirable size of the used watermark images is in the form of r×s which should be smaller than the p×q size of the cover image. In this approach, the authors introduced a form metaheuristic technique namely the cuckoo search for determining the suitable location for Multi-biometric watermarks embedding which in turn improves the watermarking characteristics namely visual quality and robustness.

5.2.4 Processing speed

The processing speed of the proposed watermarking algorithm is computed using the computational time of the embedding and extraction algorithm. It is defined as follows:

6 Embedding algorithm

- DTCWT – To obtain complex coefficients that are shift-invariance, strong directional selectivity, perfect reconstruction, limited redundancy, and low computing complexity
- Pseudo-Zernike moments and Harris corner points – To determine invariant feature points.
- Cuckoo search optimization – optimal embedding location
- Zernike moments, Arnold scrambling and SHA-128 – To provide security for watermarks
- Process of embedding - The process of embedding in the DTCWT coefficients provides more embedding capacity, which in turn promotes its visual perception. The introduc-

Table 4 Processing speed of the proposed embedding and extraction algorithm

Algorithm	Time in s
Embedding Algorithm	1.4562 s
(i) DTCWT	0.345
(ii) Pseudo-Zernike moments and Harris corner points	0.102
(iii) Cuckoo search optimization	0.354
(iv) Zernike moments, Arnold scrambling and SHA-128	0.13 + 0.15 + 0.11
(v) Process of embedding	0.2
(vi) Generation of the authentication key	0.0652
Extraction Algorithm	0.0232 s
(i) First level of authentication of watermarked image	0.0042
(ii) Multi-biometric Watermarks Detection	0.0134
(iii) Extraction of Multi-biometric Watermarks	0.0031
(iv) Next level of authentication ○ Tamper detection and Recovery and ○ Tamper detection and Fragile.	0.0025

tion of optimized embedding also improves the robustness and security of the proposed system, and

- Generation of the authentication key - To test the authenticity of the watermarked image.

7 Extraction algorithm

- First level of authentication of watermarked image,
- Multi-biometric Watermarks Detection,
- Extraction of Multi-biometric Watermarks, and
- Next level of authentication –
- Tamper detection and Recovery and
- Tamper detection and Fragile.

Thus to process the sample cover image of size 512×512, the time taken for various stages of embedding and extraction are depicted in Table 4.

The proposed processing speed is better when compared to the existing approaches due to the low computing complexity of DTCWT. Unlike Hu moments, PZM can be reconstructed using the higher order moments itself. The proposed system not only concentrates on maintaining the trade-off among visual quality, robustness, security and payload.

7.1 Attacks

The *WI* namely watermarked image might get corrupted due to either intentional or unintentional attacks by the proscribed users in the insecure network. The visual quality and the robustness measure of the proposed system for all such degraded scenarios are authenticated on the sample images *(lena, cameraman, house, jetplane, lake, Barbara, baboon,*

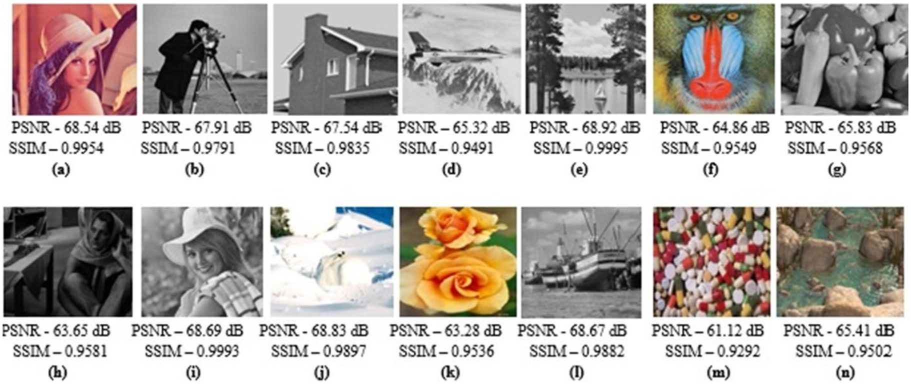


Fig. 9 Watermarked Images (**a**) *lena* (**b**) *cameraman* (**c**) *house* (**d**) *jetplane* (**e**) *lake* (**f**) *baboon* (**g**) *peppers* h) *barbara* i) *elaine* j) *arctic_hare* k) *brandyrose* l) *fishing boat* m) *pills* n) *waterfalls*

pepper) concerning the numerous attacks considerations namely: (i) Zero or No attack, (ii) Unintentional attack namely, image processing operation, geometrical, JPEG compression, and Multiple JPEG. (iii) Intentional attacks namely copy-move forgery, image splicing, cropping, and collage.

7.1.1 No or zero attack

In general, the watermark embedding itself influences the cover image's visual perception and it can be estimated efficiently by considering the watermarked image with no attack. It can be measured with the help of PSNR and SSIM metrics. Figure 9 shows the watermarked images in the "Zero Attack" and its corresponding extraction of the watermarks are presented in Fig. 10.

From Fig. 9. And Fig. 10, it is clear that the minimum PSNR we obtained is 61.12 dB for *pills* and the maximum PSNR value obtained is 68.69 dB for *elaine*, whereas, the maximum robustness factor NCC is obtained as 0.9998 and 0.9983 for *suzie* and *DS1*.

7.1.2 Unintentional attacks

a) Operations of Image Processing:

The various image processing operations are deliberated for authenticating proposed multi-biometric semi-fragile system performance are given as: (i) Image Noising – with

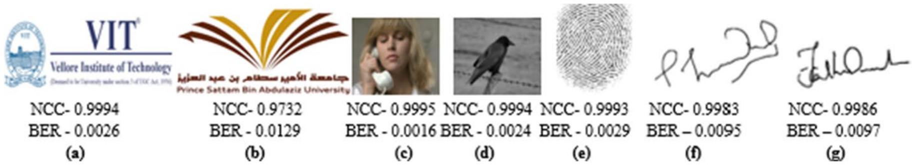


Fig. 10 Extracted Watermark Images (**a**) *VIT logo* (**b**) *PSAU logo* (**c**) *suzie* (**d**) *crow* e) *FP1* (**f**) *DS1* (g) *DS2*

variances of Gaussian noise for values 0.05, 0.1, and 0.5 respectively, with densities of Salt and pepper noise values of 0.01, 0.02 and 0.06 respectively, (ii) Image Filtering – Median filter, Average Filter, Gaussian Filter with various filter sizes of 3 * 3, 5 * 5 and 7 * 7 respectively, (iii) Compression Attack – JPEG with various quality factors of 90%, 70% and 50% and JPEG - JPEG Compression (90% - 70%, 70% - 50%, 90% - 50%). Figure 11 displays the multiple watermarks which are extracted from the above-discussed image processing attacked watermarked image.

Figure 11 clears that the proposed multi-biometric based semi-fragile system provides a higher NCC value of 0.9989 and BER value of 0.03 even at the highest quality factor value of 90 and 70 JPEG-JPEG compressions, where existing systems fail.

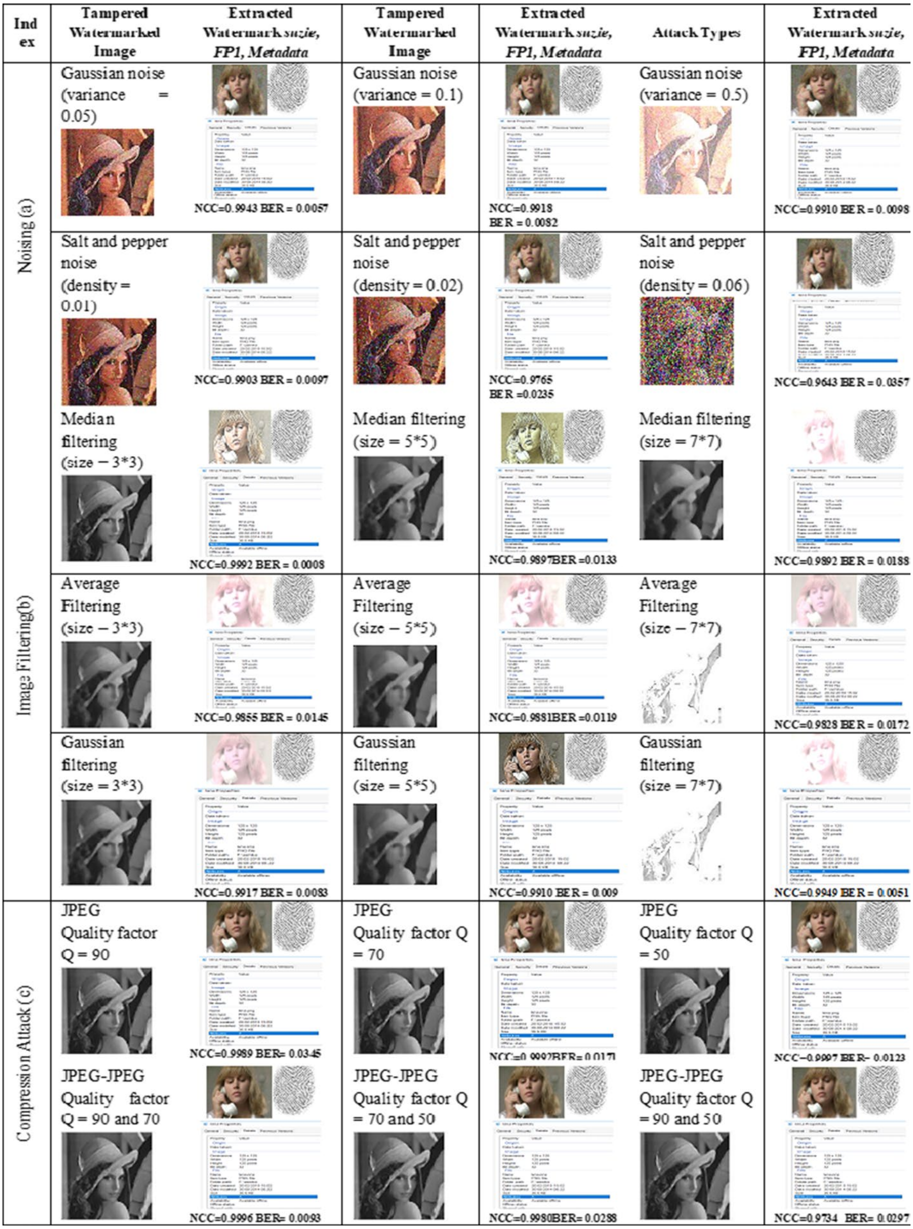
b) Geometric Attack:

This section dealt with the validation of the proposed multi-biometric based semi-fragile system against geometric attacks, where the conventional systems fail namely the RST (rotation, scaling, and translation) property. The robustness measure of the proposed system concerning RST is made with the following considerations as (i) rotation with different degrees of 10°, 25°, and 45°, and (ii) scaling with different percentages of 50%, 75%, and 125% and (iii) translation at different directions of x and y namely, $T_x = -25$ and $T_y = 10$, $T_x = -50$ and $T_y = 50$ and $T_x = 45$ and $T_y = -25$ respectively. Figure 12 exhibits degraded RST watermarked image and the extraction of corresponding multiple watermarks. From Fig. 12, we determine that the proposed multi-biometric based semi-fragile system can tolerate the rotation on the standard image *lena*, for translation and scaling on *baboon* image demonstrates the results which are good when related to the other standard test images respectively. Normally, the system becomes desynchronized due to the stated RST attacks and it is a challenging one where most conventional systems fail. To sort out this RST issue, the proposed multi-biometric system computed SVD on Pseudo Zernike Moments over Harris corner feature points in the DTCWT coefficients on the higher energy blocks. These parameters with the attacked images SSIM and NCC value and capacity are then set as input for an optimization process. As a result, an optimized location that is suitable for embedding the watermarks is determined. Accordingly, embedding the identified optimal locations overcomes the problem of desynchronization by retrieving the watermarks, especially in the case of unintentional attacks.

7.1.3 Intentional attacks

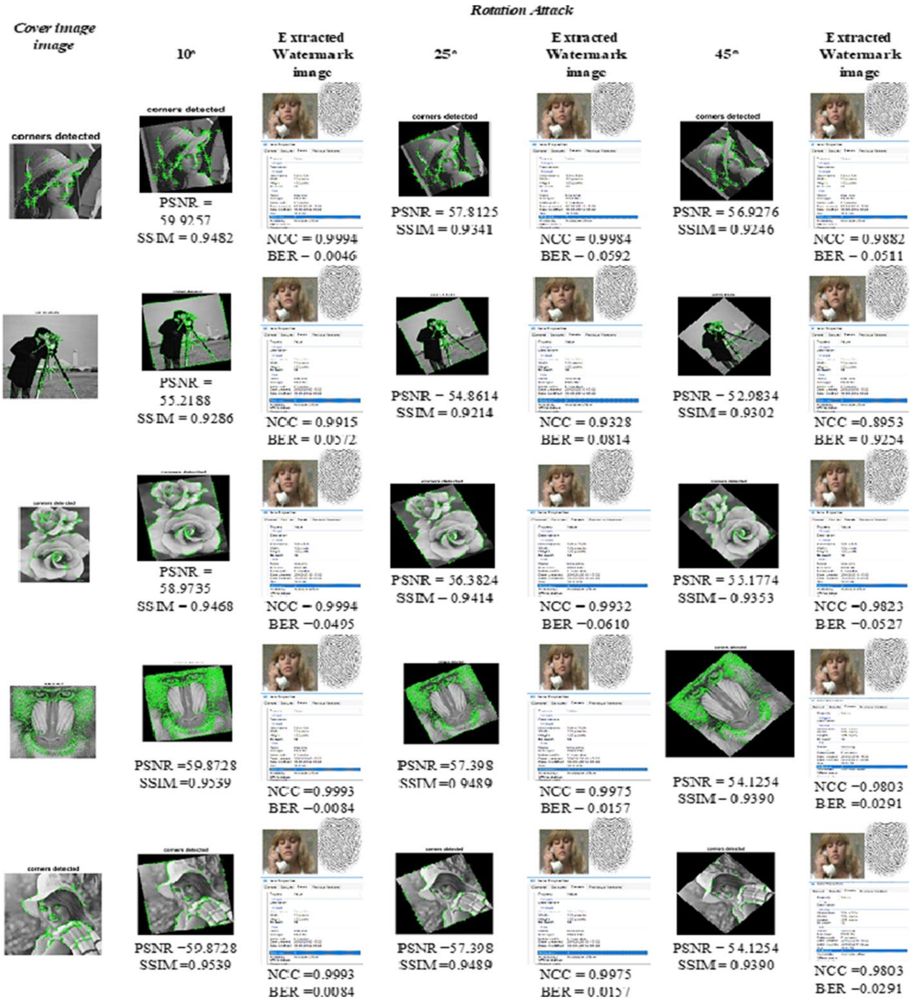
The performance of the proposed semi-fragile multi-biometric watermarking systems is evaluated using intentional attacks such as Adding, cropping, copy-move forgery, and Image Splicing. Adding in the process of adding some new information onto the image randomly. Cropping is the process of removing a part of the image. Copy move forgery is copying and placing the part of an object in an image. Image Splicing is introducing some new image or part of an image randomly. The proposed semi-fragile system can detect the tampered region and perform fragile on the watermarked image as these tampers have happened intentionally. It is shown in Fig. 13.

From the above results, it is clear that the minimum and maximum visual quality in terms of SSIM, and PSNR are 0.8855, 0.9985, and 45.9234, 68.6967 respectively. Similarly, the minimum and maximum of robustness in terms of NCC are 0.8953, and 0.9994 respectively. All these values are within the acceptable limit.



Index	Tampered Watermarked Image	Extracted Watermark *suzie, FP1, Metadata*	Tampered Watermarked Image	Extracted Watermark *suzie, FP1, Metadata*	Attack Types	Extracted Watermark *suzie, FP1, Metadata*
Noising (a)	Gaussian noise (variance = 0.05)	NCC=0.9943 BER = 0.0057	Gaussian noise (variance = 0.1)	NCC=0.9918 BER = 0.0082	Gaussian noise (variance = 0.5)	NCC=0.9910 BER = 0.0098
	Salt and pepper noise (density = 0.01)	NCC=0.9903 BER = 0.0097	Salt and pepper noise (density = 0.02)	NCC=0.9765 BER =0.0235	Salt and pepper noise (density = 0.06)	NCC=0.9643 BER = 0.0357
Image Filtering(b)	Median filtering (size – 3*3)	NCC=0.9992 BER = 0.0008	Median filtering (size = 5*5)	NCC=0.9897BER =0.0133	Median filtering (size = 7*7)	NCC=0.9892 BER = 0.0188
	Average Filtering (size – 3*3)	NCC=0.9855 BER = 0.0145	Average Filtering (size – 5*5)	NCC=0.9881BER =0.0119	Average Filtering (size – 7*7)	NCC=0.9828 BER = 0.0172
	Gaussian filtering (size = 3*3)	NCC=0.9917 BER = 0.0083	Gaussian filtering (size = 5*5)	NCC=0.9910 BER = 0.009	Gaussian filtering (size = 7*7)	NCC=0.9949 BER = 0.0051
Compression Attack (c)	JPEG Quality factor Q = 90	NCC=0.9989 BER= 0.0345	JPEG Quality factor Q = 70	NCC=0.9992BER=0.0171	JPEG Quality factor Q = 50	NCC−0.9997 BER− 0.0123
	JPEG-JPEG Quality factor Q = 90 and 70	NCC=0.9996 BER= 0.0093	JPEG-JPEG Quality factor Q = 70 and 50	NCC=0.9980BER= 0.0288	JPEG-JPEG Quality factor Q = 90 and 50	NCC=0.9734 BER= 0.0297

Fig. 11 Extraction of *suzie, FP1, Metadata* watermarks after Image Processing operations (**a**) Image Noising (**b**) Image filtering, and (**c**) JPEG Compression



(a)

Fig. 12 Geometric Attacks (**a**) Rotation, (**b**) Scaling, (**c**) Translation on sample Watermarked Images (*lena, cameraman, brandyrose, baboon, elaine*) and the Extracted Watermarks (*suzie, Receiver's fingerprint, Metadata*)

8 Comparative study

To justify the proposed system's performance, we implemented the existing tamper detection-based watermarking algorithms [24, 33], Zernike moments-based watermarking system [40, 49], Pseudo Zernike moments-based watermarking system [60], Dual-tree Complex Wavelet transform-based watermarking algorithm [63], color image watermarking [1] with the dataset used for the proposed work and the same also been compared with the introduction of various attacks. Tables 5, 6, 7, 8 and 9 depicts the interpretations during No or Zero Attack conditions, Unintentional - Image

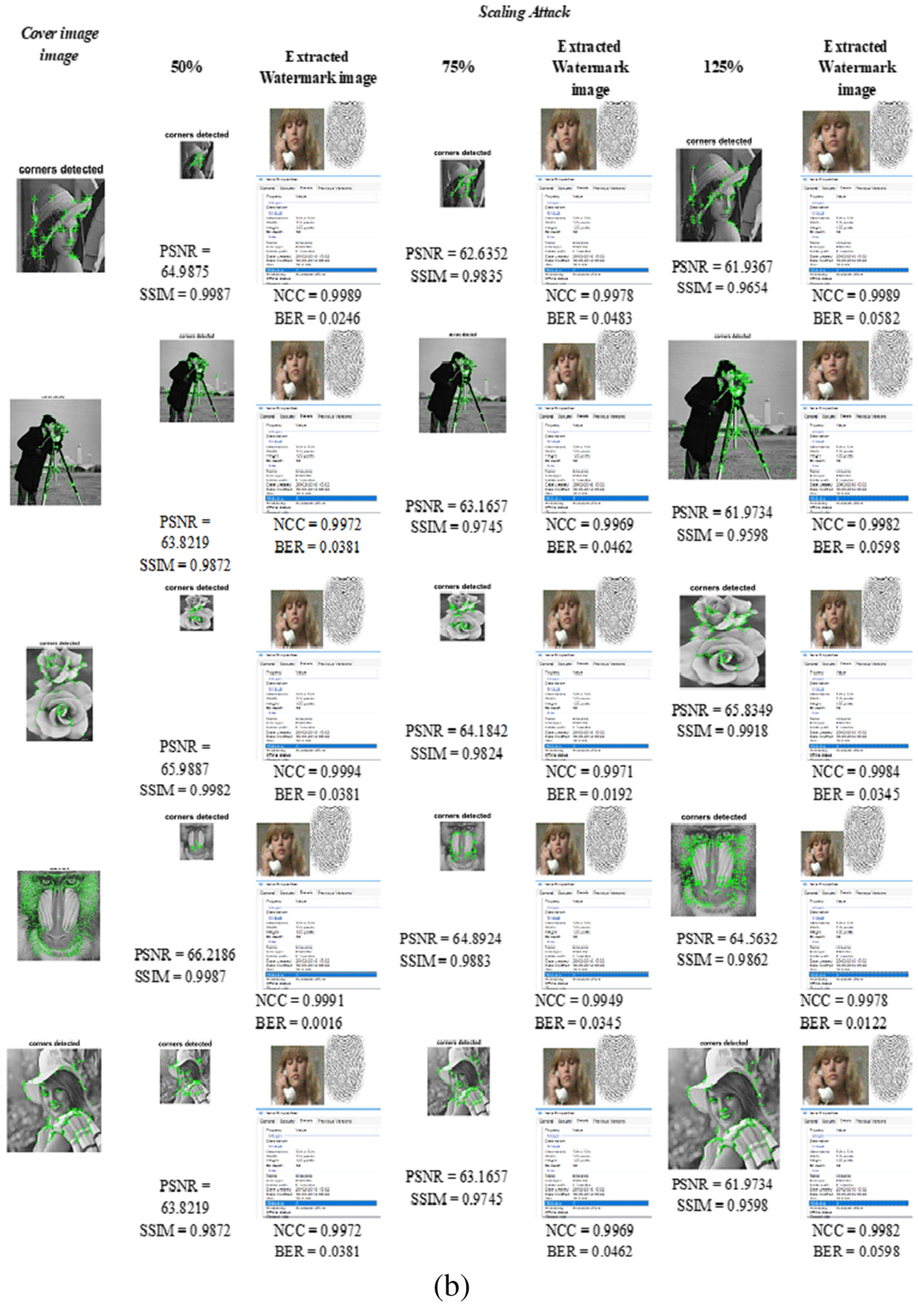


Fig. 12 (continued)

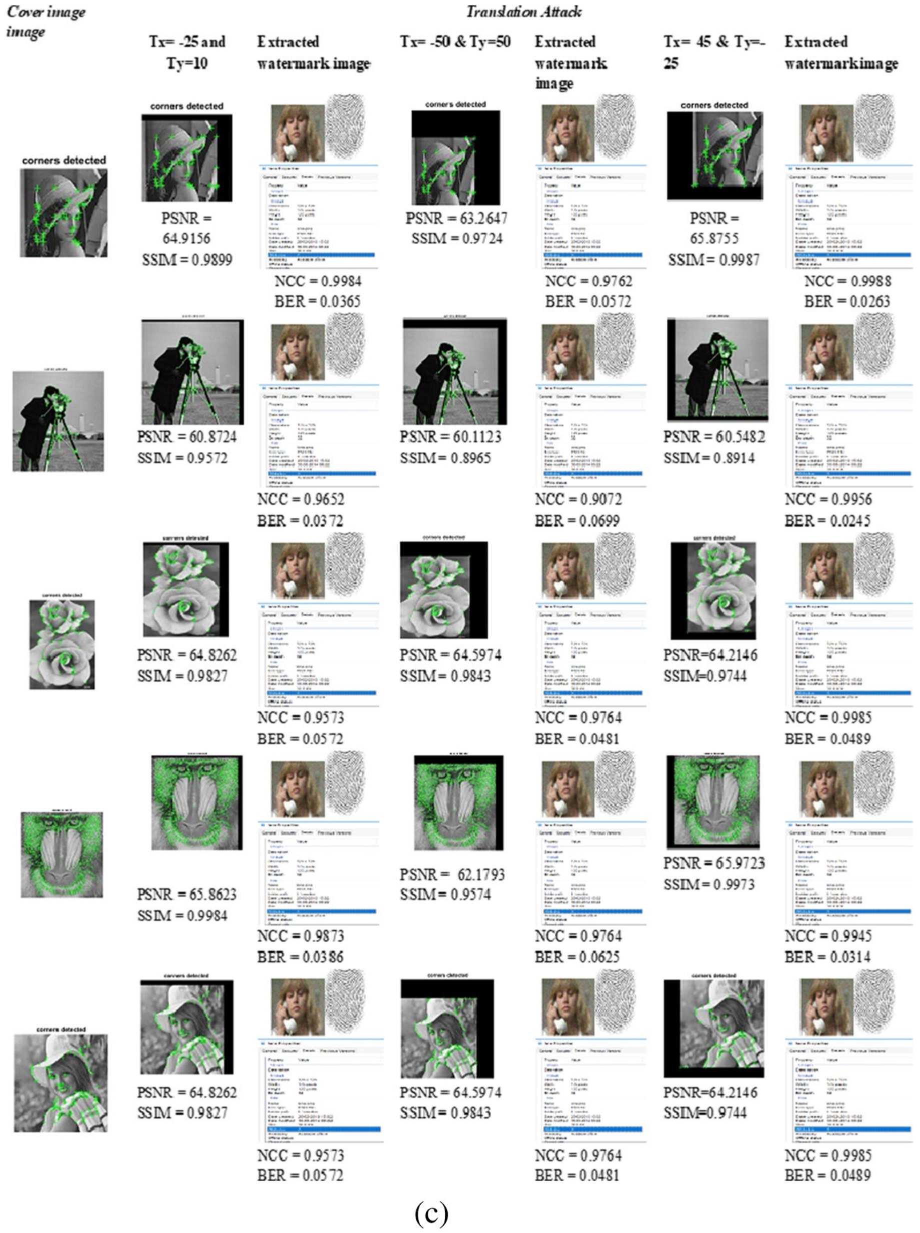


Fig. 12 (continued)

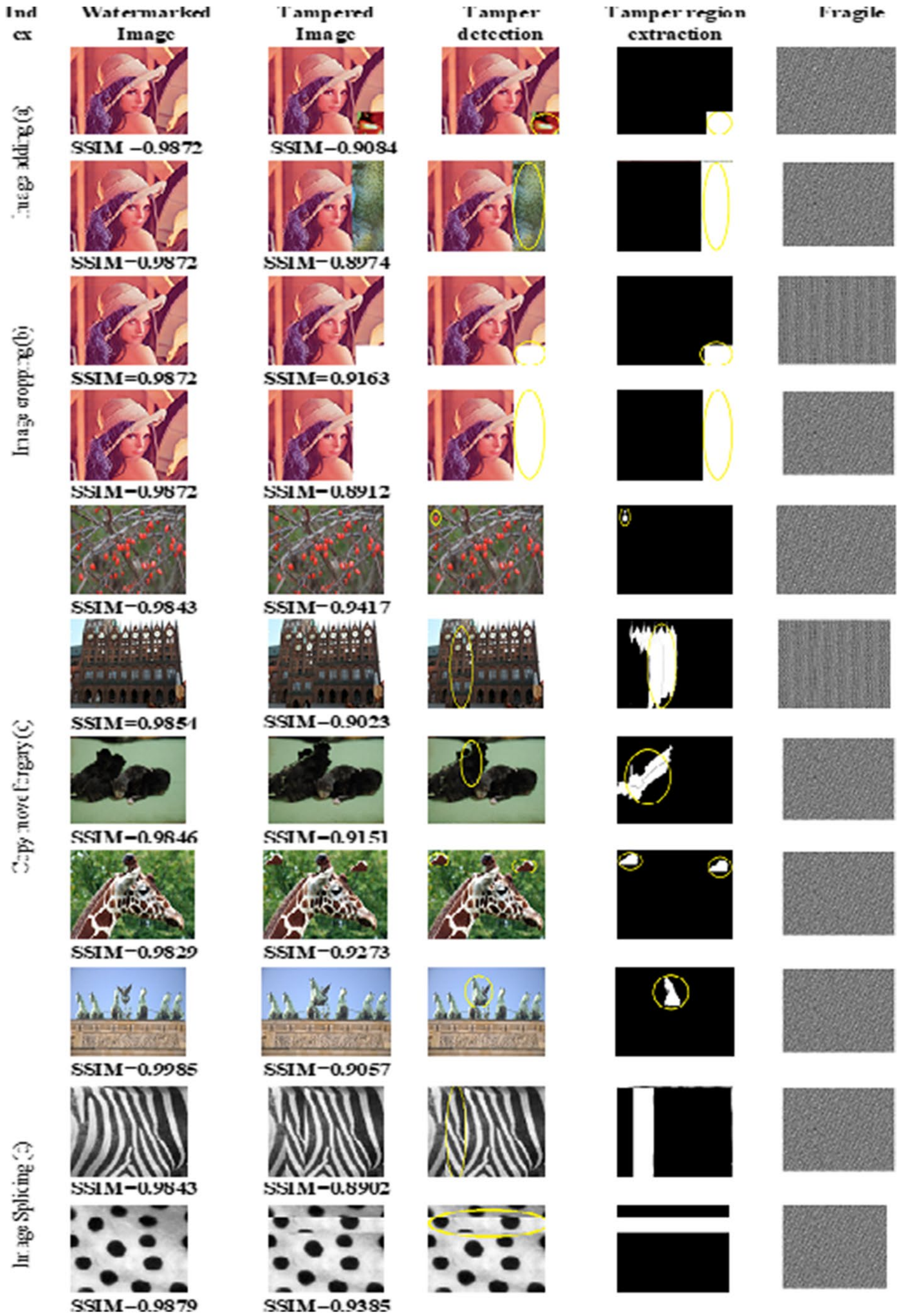


Fig. 13 Intentional Attacks – Tamper detection and fragile (**a**) Image Adding (**b**) Image cropping (**c**) Copy move forgery and (**d**) Image Splicing

processing attacks, Unintentional - Geometric attacks, Intentional Attacks and Processing speed respectively.

Table 5 clears that the proposed multi-biometric based semi-fragile watermarking system attains higher visual quality on the standard test images *lena, cameraman, baboon, elaine, and brandyrose* for the value of PSNR value when related to the conventional systems. Similarly, the robustness value of the proposed system in terms of NCC is obtained as 0.999 which is very great when related to the other state-of-the-art approaches. Also, Zebbiche et al. [63] achieves an NCC value of about 0.9892 which is the next better one after the proposed multi-biometric based semi-fragile watermarking system.

The proposed multi-biometric based semi-fragile watermarking system that is vulnerable to various unintentional and intentional attacks in terms of imperceptibility and robustness is tested and related to the relevant watermarking systems and the same are depicted in the following Tables 6, 7 and 8.

The first test is conducted using image processing operations namely Noising on Image due to G with the values of variance such as 0.05, 0.1, and 0.5, SP with various densities of noise such as 0.01, 0.02, and 0.06, Filtering on Image with various filter sizes 3*3, 5*5 and 7*7 using MF, AF, and GF, compression on Image namely JPEG with the various quality factors of 90%, 70% and 50%, JPEG-JPEG Compression with the combined quality factors of 90% and 70%, 70% and 50%, and 90% and 50% respectively.

The outcomes précised in Table 6 dissipates that the proposed multi-biometric based semi-fragile watermarking system can extract 99.34%, 98.63%, 98.94%, 98.86%, 99.32%, 99.16%, and 98.64% on an average of multiple watermarks when the images are affected by G, SP, MF, AF, GF, JPEG, and JPEG - JPEG respectively. From the outcomes displayed in Table 6, we infer that the multi-biometric based semi-fragile watermarking system can tolerate various image processing operations superior to the related conventional watermarking systems. Table 6 also depicts that the proposed system is very much robust against median filtering (M) of 3*3, JPEG (50%), and JPEG-JPEG (70 and 50%) with an NCC value of 0.9942, 0.9995, and 0.9994 respectively concerning the other image processing operations. Particularly, the watermark extraction rate is approximately 99.16% when the watermarked images are degraded by G whose variance is 0.1.

During the second experiment, the watermarked image sequences get affected by geometrical distortions namely RST (Rotation, Scaling, and Translation). The various rotation degrees considered are 5°, 15°, 45°, 70°, and 90°, scaling percentages are 50%, 90%, 120%, 150%, 200% and 300% and parameters of translation parameters are $T_x = -25$and $T_y = 10$, $T_x = -50$ and $T_y = 50$, and $T_x = 45$ and $T_y = -25$ respectively for better experiment.

Table 7 compares the correlation coefficient among the proposed multi-biometric system with the existing systems under various geometric conditions. The average watermarks extraction is obtained as 98% for rotation, 99%, for scaling, and 98% for translation respectively.

Figure 14 delivers that the results of the proposed system were found upright while compared to the existing state – of – the – art systems in terms of watermark detection and extraction namely NCC.

In the third experiment, the influence of various intentional attacks on the proposed and existing systems are evaluated namely, image cropping, copy-move forgery, and image splicing with the existing algorithm by Behrouz et al., 2019 [24]. From Table 8, we conclude that the watermark extraction works well on all forms of image cropping, copy-move forgery, and splicing. The proposed approach can extract 99.4%, 99.2%, 99.1%, 99.6%, 99.3%, 97.9%, and 99.4% of watermark when the images are cropped randomly at the rate

Table 5 No Attack

Benchmark dataset/ Metrics	Ours		[33]	[1]	[63]	[60]	[24]	[40]	[49]
Lena	PSNR	68.54	45.32	42.23	62.63	46.24	46.45	46.26	40.92
	SSIM	0.9995	0.9987	0.9742	0.9882	0.9984	0.9987	0.9980	0.9752
	NCC	0.9998	0.9908	0.9793	0.9892	0.9813	0.9746	0.9782	0.9763
Cameraman	PSNR	67.41	46.30	41.45	60.12	45.85	45.80	46.81	41.63
	SSIM	0.9994	0.9979	0.9783	0.9875	0.9987	0.9976	0.9984	0.9767
	NCC	0.9991	0.9938	0.9754	0.9817	0.9542	0.9742	0.9715	0.9834
Baboon	PSNR	64.86	40.31	40.82	59.43	47.01	45.79	46.20	40.71
	SSIM	0.9989	0.9954	0.9724	0.9863	0.9989	0.9974	0.9981	0.9772
	NCC	0.9983	0.9503	0.9737	0.9802	0.9883	0.9829	0.9813	0.9658
Elaine	PSNR	68.69	44.26	42.54	61.23	46.48	45.78	46.87	41.78
	SSIM	0.9998	0.9983	0.9776	0.9877	0.9987	0.9975	0.9985	0.9798
	NCC	0.9995	0.9463	0.9799	0.9873	0.9831	0.9852	0.9722	0.9795
Brandyrose	PSNR	63.28	48.854	41.96	58.37	45.74	45.39	46.02	40.75
	SSIM	0.9996	0.9985	0.9774	0.9852	0.9986	0.9970	0.9982	0.9761
	NCC	0.9894	0.9541	0.9846	0.9812	0.9693	0.9842	0.9761	0.9722

Table 6 The Image Processing attacks Between the proposed and the existing approaches on 'lena'

Type of Attacks	[63]	[60]	[24]	[40]	[49]	[33]	[1]	Ours
	NCC	NCC	NCC	NCC	NCC	NCC	NCC	NCC
Gaussian of variance 0.05	0.9564	0.9490	0.9654	0.9389	0.9057	0.9356	0.9039	0.9942
Gaussian of variance 0.1	0.9534	0.9217	0.9143	0.9264	0.8863	0.9311	0.9012	0.9916
Gaussian of variance 0.5	0.9271	0.9099	0.9327	0.9157	0.9143	0.9245	0.9011	0.9913
Salt and Pepper with density 0.01	0.9947	0.9584	0.9816	0.9193	0.885	0.9132	0.8942	0.9906
Salt and Pepper with density0.02	0.9638	0.9575	0.9645	0.9075	0.876	0.9124	0.8854	0.9867
Salt and Pepper with density 0.06	0.9562	0.9526	0.9571	0.8796	0.862	0.9035	0.8746	0.9755
Median filter of size 3*3	0.9961	0.9621	0.9883	0.9681	0.8214	0.9442	0.9654	0.9993
Median filter of size 5*5	0.9896	0.9642	0.9877	0.9278	0.8176	0.9455	0.9748	0.9889
Median filter of size 7*7	0.9863	0.9673	0.9643	0.9112	0.7999	0.9473	0.9856	0.9893
Average filter of size3*3	0.9941	0.9671	0.9864	0.9409	0.8160	0.9654	0.9532	0.9854
Average filter of size 5*5	0.988	0.9488	0.9757	0.9218	0.8023	0.9577	0.9553	0.9879
Average filter of size7*7	0.9899	0.9325	0.9861	0.9136	0.7935	0.9583	0.9562	0.9897
Gaussian filter of size 3*3	0.9993	0.9689	0.9882	0.9581	0.8952	0.9634	0.9694	0.9921
Gaussian filter of size5*5	0.9976	0.9437	0.9756	0.9376	0.8913	0.9543	0.9598	0.9924
Gaussian filter of size 7*7	0.9574	0.9388	0.9582	0.9299	0.8762	0.9419	0.9512	0.9952
JPEG with QF 90%	0.9433	0.9782	0.9345	0.9699	0.8754	0.9575	0.9961	0.9991
JPEG with QF 70%	0.9538	0.9693	0.9782	0.9672	0.8566	0.9454	0.8941	0.9993
JPEG with QF50%	0.9623	0.9654	0.9692	0.9323	0.8382	0.9242	0.8774	0.9995
JPEG – JPEG (90 and 70%)	0.9342	0.9864	0.9453	0.9532	0.8684	0.9543	0.9532	0.9978
JPEG – JPEG (70 and 50%)	0.9584	0.9943	0.9627	0.9524	0.8434	0.9375	0.9348	0.9994
JPEG – JPEG (90 and 50%)	0.9236	0.9549	0.9613	0.9323	0.8325	0.9452	0.9243	0.9974

Table 7 The Geometrical Attacks Between the Proposed and the existing Approaches on ‘lena’

Type of Attacks		[63] NCC	[60] NCC	[24] NCC	[40] NCC	[49] NCC	[33] NCC	[1] NCC	Ours NCC
Rotation	(5°)	0.9887	0.9864	0.967	0.988	0.9864	0.9345	0.9143	0.9984
	(15°)	0.9838	0.9781	0.962	0.9816	0.9781	0.9301	0.9121	0.9974
	(25°)	0.9812	0.9463	0.9547	0.9735	0.9463	0.9254	0.9094	0.9884
	(45°)	0.9754	0.9275	0.9523	0.9612	0.9275	0.9232	0.9043	0.9892
	(70°)	0.9719	0.8682	0.8617	0.8932	0.8682	0.9214	0.8995	0.9891
	(90°)	0.9893	0.8578	0.8953	0.9256	0.8578	0.9335	0.8974	0.9997
Scaling	(50%)	0.9238	0.9984	0.886	0.928	0.9984	0.9444	0.9465	0.9989
	(75%)	0.9967	0.9962	0.8812	0.9154	0.9962	0.9545	0.9448	0.9978
	(125%)	0.9987	0.9546	0.8673	0.9011	0.9546	0.9447	0.9456	0.9989
	(150%)	0.9997	0.9335	0.8325	0.8874	0.9335	0.9416	0.9432	0.9997
	(200%)	0.9993	0.9281	0.8198	0.8815	0.9281	0.9357	0.9454	0.9997
	(300%)	0.9946	0.9092	0.811	0.8597	0.9092	0.9315	0.9368	0.9974
Translation	$T_X = -25$ AND $T_Y = 10$	0.9834	0.9658	0.8989	0.9528	0.9152	0.9357	0.9496	0.9988
	$T_x = -50$ and $T_y = 50$	0.9762	0.9443	0.8956	0.9437	0.9134	0.9345	0.9442	0.9976
	$T_X = -50$ AND $T_Y = -45$	0.9543	0.9328	0.8924	0.9329	0.9076	0.9284	0.9342	0.9965

Table 8 The Intentional Attack between the Proposed and Existing Approach

Type of Attacks	Behrouz et al., 2019 [24]	Pascal et al., 2022 [33]	Ours
	NCC	NCC	NCC
Image Cropping (10%)	0.9923	0.9452	0.9946
Image Cropping (25%)	0.9901	0.9423	0.9927
Copy move forgery (object)	0.9900	0.9389	0.9915
Copy move forgery (background)	0.9859	0.9367	0.9968
Image Splicing (horizontal)	0.9831	0.9302	0.9931
Image Splicing (vertical)	0.9820	0.9366	0.9792
Image Splicing (corner)	0.9939	0.9587	0.9947

of 10%, 25%, copy-move forgery on an object, on the background and image splicing at the horizontal level, vertical level, corner level respectively. All these obtained correlation coefficient proves that the proposed system works superior to the existing system [24] (Table 8).

Finally, the processing speed (average CPU time) of the proposed system is compared with the related existing systems and it is depicted in Table 9. From the table, it is evident that the proposed approach takes comparatively more time to perform embedding and extraction algorithm than other similar transforms. This is mainly because, in the existing systems only a single form of transforms are performed, but the proposed system involves PZM, Security algorithms on multiple watermarks in addition to the use of complex numbers in the DTCWT structure. It is, however, because every component in our proposed

Table 9 The Processing Speed between the Proposed and Existing Approaches

Approaches	Embedding Algorithm *(s)*	Extraction Algorithm *(s)*
Ours	1.4562	0.0232
DTCWT [32]	1.6766	0.0269
DTCWT [15]	0.6241	0.5668
DWT [9]	0.2094	0.6481

system is performed sequentially and separately. Therefore, these processes can also be executed in parallel to speed up the process. On the other hand, it can be seen that the extraction algorithm of the proposed system is significantly faster than [32] and other existing systems. It is vital to note in this situation that the extraction process is more essential than embedding as it may also be done offline.

From the above experiments, it is clear that the proposed multi-biometric semi-fragile based watermarking systems are strong and provides good accuracy against various degradations caused due to unintentional image processing operations and intentional copy-move forgery, splicing, and dropping when related to the existing systems. The watermark capacity or payload is also increased sensibly in the proposed system by embedding the DTCWT coefficients on the cover image. Thus, the proposed system is the greatest fit, particularly for image authentication-based applications such as image transmission over insecure online social networks, where there is a more possibility of intentional and unintentional attacks.

9 Conclusions and future scope

The multi-biometric semi-fragile based watermarking system for the authentication of contents using the optimized Dual-Tree Complex Wavelet Transform (DTCWT) and Pseudo Zernike moments that secure digital transmission over insecure online social networks (OSNs) is introduced in this paper. This work mainly focuses on the severity of the attacked watermarked content which is normally suffering from intentional and unintentional attacks. Based on the severity of the tampering, either tamper detection and

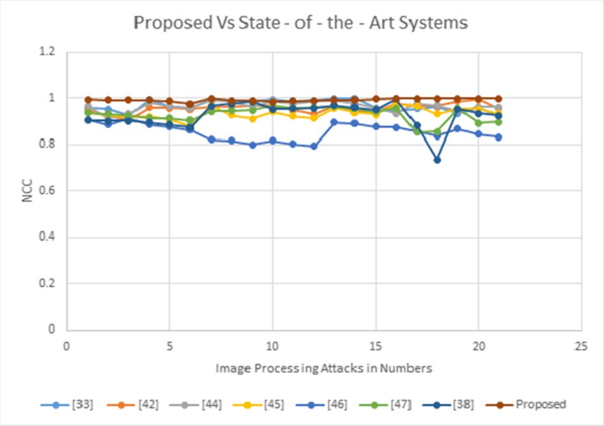


Fig. 14 Proposed Vs State-of-the-art systems (Image Processing Attacks)

recovery or tamper detection and fragile are performed particularly for attacks namely JPEG compression, rotation, scaling, translation, copy-move forgery, image splicing, and cropping. It should be noted that most existing systems are unsuccessful to resist all such attacks. The proposed image watermarking technique uses nature-inspired watermarking over the pseudo-Zernike moments of the Harris corner points in the DTCWT domain to decide the optimum embedding location. The proposed system's innovation is elaborated as: The DTCWT coefficients are used for content authentication by expressing the digital images in the transform domain. The Pseudo-Zernike moments of the Harris corner points which are detected on DTCWT coefficients make the system attain high robustness level against geometric attacks namely scaling and rotation when compared to the conventional systems. The SVD's property of invariant to translation makes the system resist translation. Hence, the system which is proposed achieves RST invariant.

The four-level of Authentication and its security are accomplished by the owner's digital signature, randomizing the multiple watermark images using Zernike moments, Arnold transforms and SHA algorithm respectively. The metaheuristic approach for finding the location suitable for embedding is calculated using Cuckoo search optimization using multiple objective function parameters one comprises of namely, SSIM for visual quality, correlation coefficient, and Capacity, and the other comprises false positive, false negative probabilities, and squared Euclidean distance between extracted PZM and regenerated PZM respectively. Then, on the acquired optimal location for embedding, the SVD is performed and leads to obtaining the modified singular values. The inverse SVD and DTCWT computation has resulted in the watermarked image. This system achieves four-level authentications, the first level is obtained by the extracted watermark images decryption with the help of an appropriate key and the other is attained by equating the key which is regenerated with the extracted one. The third level authentication is achieved using decrypted fingerprint with the receiver's fingerprint and finally, fourth level authentication is performed. If the resultant similarity is greater than the T_A threshold value, then validation is assumed to be a success. Otherwise, the watermarked image which is received is not an authenticated one, so the next level of authentication is performed by comparing the extracted PZM with the regenerated PZM to determine the severity of damage that happened either due to intentional or unintentional activities. Recalling the challenges given in Section 2, the need for determining the action to be taken under various attacks and RST invariant property due to the desynchronization caused during geometrical attacks has been experimentally highlighted for online social media data and we have provided the solution for the same.

Though the proposed system concentrates mainly on content authenticity, it also retains the trade-off between visual quality, capacity, and robustness when compared to the existing tamper detection and recovery-based watermarking systems. It clears from the maximum PSNR and NCC of about 68 dB and 0.9995 respectively. In nutshell, the proposed multi-biometric based semi-fragile watermarking system is appropriate for content authentication applications of online social media data when compared to the existing approaches. The shortcomings of the proposed system is defined as an extraction can only be performed with the supportive information of the encoder which is used for embedding and termed non-blind. These systems won't be suitable for asynchronous transmission, where embedding and extraction happen independently. The extension of this system is possible by incorporating the semi-fragile blind watermarking form. Thus, the extraction process does not require any side information which makes the system to be computationally effective. In addition, to improve the processing speed of the proposed system, a typical parallelism can be applied on each stages of embedding and extraction process.

Acknowledgements The authors extend their sincere thanks to PSAU – College of Engineering, Saudi Arabia for funding this work through the New Faculty Grant Program under grant number (2018/01/9362) and Vellore Institute of Technology, Vellore, India for providing space to carry out this work successfully.

Funding This work is funded by PSAU – College of Engineering, Saudi Arabia through the New Faculty Grant Program under grant number (2018/01/9362).

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest There is no Conflict of Interest or competing interests by the authors.

References

1. Abadi RY, Moallem P (2022) Robust and optimum color image watermarking method based on a combination of DWT and DCT. Optik 261:169146
2. Abdulla, AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Doctoral thesis, University of Buckingham
3. Agbaje, M, Awodele O, Ogbonna C (2015) "Applications of digital watermarking to cyber security (cyber watermarking)," In Proceedings of Informing Science & IT Education Conference (InSITE), pp. 1–11
4. Agilandeeswari L, Ganesan K (2016) A bi-directional associative memory based multiple image watermarking on cover video. Multimed Tools Appl 75(12):7211–7256
5. Agilandeeswari L, Ganesan K (2016) A robust color video watermarking scheme based on hybrid embedding techniques. Multimed Tools Appl 75(14):8745–8780
6. Agilandeeswari L, Ganesan K (2016) An efficient Hilbert and integer wavelet transform based video watermarking. J Eng Sci Technol 11(3):327–345
7. Agilandeeswari L, Ganesan K (2016) False-positive free Hilbert and multi-resolution-based image watermarking technique using firefly optimisation algorithm. Int J Inf Privacy, Security Integr 2(4):257–280
8. Agilandeeswari L, Ganesan K (2018) RST invariant robust video watermarking algorithm using quaternion curvelet transform. Multimed Tools Appl 77(19):25431–25474
9. Agilandeeswari, Loganathan, and Kumaravel Muralibabu,"A Robust video watermarking algorithm for content authentication using discrete wavelet transform (DWT) and singular value decomposition (SVD)," Int J Secur Appl,vol.7, no. 4, pp.145–158, 2013.
10. Agilandeeswari L, Ganesan K, Muralibabu K (2013) A side view based video in video watermarking using DWT and Hilbert Transform. In: Thampi SM, Atrey PK, Fan CI, Perez GM (eds) Security in Computing and Communications. SSCC 2013. Communications in Computer and Information Science, vol 377. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40576-1_36
11. Ahvanooey MT, Li Q, Zhu X, Alazab M, Zhang J (2020) ANiTW: a novel intelligent text watermarking technique for forensic identification of spurious information on social media. Comput Secur 90:101702
12. Ali M, Ahn CW, Pant M (2014) Cuckoo search algorithm for the selection of optimal scaling factors in image watermarking, In Proceedings of the Third International Conference on Soft Computing for Problem Solving, pp. 413–425. Springer, New Delhi
13. Alsmirat MA, Jararweh Y, Obaidat I et al (2017) Automated wireless video surveillance: an evaluation framework. J Real-Time Image Proc 13:527–546
14. Amerini I, Ballan L, Caldelli R et al (2011) a sift-based forensic method for copy–move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur 6(3):1099–1110
15. Asikuzzaman M, Alam MJ, Lambert AJ, Pickering MR (2014) Imperceptible and robust blind video watermarking using chrominance embedding: a set of approaches in the DT CWT domain. IEEE Trans Inf Forensics Secur 9(9):1502–1517
16. Belkasim SO, Shridhar M, Ahmadi M (1991) Pattern recognition with moment invariants: a comparative study and new results. Pattern Recogn 24(12):1117–1138
17. Benyoussef M, Mabtoul S, El Marraki M, Aboutajdine D (2014) Robust image watermarking scheme using visual cryptography in dual-tree complex wavelet domain. J Theor Appl Inf Technol 60(2):372–379
18. Bosher H, Yeşiloğlu S (2019) An analysis of the fundamental tensions between copyright and social media: the legal implications of sharing images on Instagram. Int Rev Law, Comput Technol 33(2):164–186

19. Cardoso P, Hawk DV, Cross D (2020) What young people need to make better-informed decisions when communicating with digital images: implications for mental health and well-being. Health Educ Behav 47(1):29–36
20. Chen C-H, Tang Y-L, Wang C-P, Hsieh W-S (2014) A robust watermarking algorithm based on salient image features. Optik 125(3):1134–1140
21. Chen S, Su Q, Sun Y, Zhang X (2022) A blind color image watermarking algorithm using the energy concentration principle of Hadamard matrix. Optik 249:168231
22. Domingo-Ferrer, J (2011) "Rational enforcement of digital oblivion," In Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society, pp. 1–8
23. Gadicha, AB, Gupta, VBB, Gadicha, VB, et al (2021) Multimode approach of data encryption in images through quantum steganography. In Multidisciplinary approach to modern digital steganography (pp. 99–124). IGI Global
24. Haghighi BB, Taherinia AH, Mohajerzadeh AH (2019) TRLG: fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA. Inf Sci 486:204–230
25. Hossain MS, Alhamid MF, Muhammad G (2018) Collaborative analysis model for trending images on social networks. Futur Gener Comput Syst 86:855–862
26. Hsu, Y-F, Chang S-F (2006) Detecting image splicing using geometry invariants and camera characteristics consistency. international conference on multimedia and expo,09-12 July 2006, Toronto, ON, Canada, pp. 549–552.
27. Huang H-C, Chu C-M, Pan J-S (2009) The optimized copyright protection system with genetic watermarking. Soft Comput 13(4):333–343
28. Kingsbury N (2001) Complex wavelets for shift invariant analysis and filtering of signals. Appl Comput Harmon Anal 10(3):234–253
29. Koppanati RK, Kumar K (2020) P-MEC: polynomial congruence-based multimedia encryption technique over cloud. IEEE Consum Electron Mag 10(5):41–46
30. Koppanati, RK, Qamar, S, Kumar, K (2018) SMALL: secure multimedia technique using logistic and LFSR. In 2018 second international conference on intelligent computing and control systems (ICICCS) (pp. 1820–1825). IEEE
31. Koppanati RK, Kumar K, Qamar S (2019) E-MOC: an efficient secret sharing model for multimedia on cloud. In: International conference on deep learning, artificial intelligence and robotics. Springer, Cham, pp 246–260
32. Kwitt R, Meerwald P, Uhl A (2009) Blind DT-CWT domain additive spread-spectrum watermark detection. In: proceedings of the 16th international conference on digital signal processing, pp 1–8
33. Lefèvre P, Carré P, Fontaine C, Gaborit P, Huang J (2022) Efficient image tampering localization using semi-fragile watermarking and error control codes, Signal Processing. 190:108342. https://doi.org/10.1016/j.sigpro.2021.108342
34. Li F, Kui W, Lei J et al (2016) Steganalysis over large-scale social networks with high-order joint features and clustering ensembles. IEEE Trans Inf Forensics Secur 11(2):344–357
35. Li J, Yu C, Gupta BB et al (2018) Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. Multimed Tools Appl 77:4545–4561. https://doi.org/10.1007/s11042-017-4452-0
36. Liu X, Eskicioglu AM (2003) elective encryption of multimedia content in distribution networks: challenges and new directions. IASTED communications, internet & information technology (CIIT), USA
37. Loganathan A, Kaliyaperumal G (2016) An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system. Expert Syst Appl 63:412–434
38. Loo, P, Kingsbury N (2000) “Digital watermarking with complex wavelets,” In: Proceedings of the IEEE international conference on image processing, ICIP 2000, pp 29–32
39. Luo, W, Liu J, Liu J, Fan C (2009) "An analysis of security in social networks," In 2009 eighth IEEE international conference on dependable, autonomic and secure computing, pp. 648–651. IEEE
40. Lutovac B, Daković M, Stanković S et al (2017) An algorithm for robust image watermarking based on the DCT and Zernike moments. Multimed Tools Appl 76(22):23333–23352
41. Meet People on Badoo, Make New Friends, Chat, Flirt, (2017) [Online]. Available: http://www.badoo.com, Accessed 04 April 2017
42. Moad MS, Kafi MR, Khaldi A (2022) A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocess Microsyst 90:104490
43. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2018) Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Futur Gener Comput Syst 86:951–960

44. Patsakis C, Zigomitros A, Papageorgiou A, Galván-López E (2014) Distributing privacy policies over multimedia content across multiple online social networks. Comput Netw 75:531–543
45. Purohit K, Kumar A, Upadhyay M, Kumar K (2020) Symmetric key generation and distribution using Diffie-Hellman algorithm. In: Soft computing: theories and applications. Springer, Singapore, pp 135–141
46. Rathore S, Sharma PK, Loia V, Jeong Y-S, Park JH (2017) Social network security: issues, challenges, threats, and solutions. Inf Sci 421:43–69
47. Selesnick IW, Baraniuk RG, Kingsbury NC (2005) The dual-tree complex wavelet transform. IEEE Signal Process Mag 22(6):123–151
48. Sharma S, Kumar K (2018) GUESS: genetic uses in video encryption with secret sharing. In proceedings of 2nd international conference on computer vision & image processing (pp. 51–62). Springer, Singapore
49. Shojanazeri H, Adnan WAW, Ahmad SMS, Rahimipour S (2017) Authentication of images using Zernike moment watermarking. Multimed Tools Appl 76(1):577–606
50. Singh AK, Kumar B, Singh SK, S. P. (2018) Ghrera, and Anand Mohan,"multiple watermarking technique for securing online social network contents using back propagation neural network,". Futur Gener Comput Syst 86:926–939
51. Son, YH, You BJ, Sang-Rok O et al (2003) Affine-invariant image normalization for Log-Polar Images using momentums.In Proceedings of the 2002 international conference on control, automation, and systems (ICCAS 2003), pp. 1140–1145, Gyeongju, Korea
52. Stokes, K, Carlsson N (2013) "A peer-to-peer agent community for digital oblivion in online social networks," In 2013 eleventh annual conference on privacy, security and trust, pp. 103–110. IEEE
53. Su, Q, Liu, D, Sun, Y (2022) A robust adaptive blind color image watermarking for resisting geometric attacks. Inf Sci
54. Symantec, Internet Security Threat Report, (2017) [Online]. Available: https: //www.symantec.com/content/dam/Symantec/docs/reports/istr-21-2016-en.pdf. Accessed on: April 4, 2017.
55. Teh C-H, Chin RT (1988) On image analysis by the methods of moments. IEEE Trans Pattern Anal Mach Intell 10(4):496–513
56. Thongkor, K, Mettripun N, Pramoun T, Amornraksa T (2013) "Image watermarking based on DWT coefficients modification for social networking services," In 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, pp. 1–6. IEEE
57. Velazquez-Garcia L, Cedillo-Hernandez A, Cedillo-Hernandez M, Nakano-Miyatake M, Perez-Meana H (2022) Imperceptible–visible watermarking for copyright protection of digital videos based on temporal codes. Signal Process Image Commun 102:116593
58. Venkatachalam N, Anitha R (2017) A multi-feature approach to detect Stegobot: a covert multimedia social network botnet. Multimed Tools Appl 76(4):6079–6096
59. Venkataramana A, Ananth Raj P (2007) Image watermarking using Krawtchouk moments. In 2007 international conference on computing: theory and applications (ICCTA’07), Kolkata, India
60. Wang X-Y, Hou L-M (2010) A new robust digital image watermarking based on Pseudo-Zernike moments. Multidim Syst Sign Process 21(2):179–196
61. Yang, X-S, Deb S (2009) Cuckoo search via Lévy flights. In 2009 world congress on nature & biologically inspired computing (NaBIC), pp. 210–214. IEEE
62. Yang X-S, Deb S (2010) Engineering optimisation by cuckoo search. Int J Math Model Numer Optim 1(4):330–343
63. Zebbiche K, Khelifi F, Loukhaoukha K (2018) Robust additive watermarking in the DTCWT domain based on perceptual masking. Multimed Tools Appl 77(16):21281–21304
64. Zhang Z, Gupta BB (2018) Social media security and trustworthiness: overview and new direction. Futur Gener Comput Syst 86:914–925
65. Zigomitros, A, Papageorgiou A, Patsakis C (2012) Social network content management through watermarking, In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications, pp. 1381–1386. IEEE

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

L. Agilandeeswari[1] · M. Prabukumar[1] · Farhan A Alenizi[2]

✉ M. Prabukumar
mprabukumar@vit.ac.in

L. Agilandeeswari
agila.l@vit.ac.in

Farhan A Alenizi
fa.alenizi@psau.edu.sa

[1] School of Information Technology and Engineering (SITE), Vellore Institute of Technology, Vellore 632014, India

[2] Department of Electrical Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia