Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-018-1161-0

ORIGINAL RESEARCH

Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique

K. Shankar[1] · Mohamed Elhoseny[2] · R. Satheesh Kumar[3] · S. K. Lakshmanaprabu[4] · Xiaohui Yuan[5]

Received: 2 August 2018 / Accepted: 1 December 2018

Abstract

Secret Image Sharing (SIS) scheme is to encrypt a secret image into 'n' specious shadows. It is unable to reveal any data on the secret image if at least one of the shadows is not achieved. In this paper, wavelet-based secret image sharing scheme is proposed with encrypted shadow images using optimal Homomorphic Encryption (HE) technique. Initially, Discrete Wavelet Transform (DWT) is applied on the secret image to produce sub bands. From this process, multiple shadows are created, encrypted and decrypted for each shadow. The encrypted shadow can be recovered just by choosing some subset of these 'n' shadows that makes transparent and stack over each other. To improve the shadow security, each shadow is encrypted and decrypted using HE technique. For the concern on image quality, the new Oppositional based Harmony Search (OHS) algorithm was utilized to generate the optimal key. From the analysis, it shows that the proposed scheme provide greater security compared to other existing schemes.

Keywords Secret image sharing · Shadow · Homomorphic encryption · Discrete wavelet transform · Harmony search (OHS) algorithm · PSNR

1 Introduction

The data security is a one-in-everything preeminent squeezing issue for which few analysts investigated in depth to have an overview about it (Rani and Mary 2016). The security of change in the shrouded information can be retrieved through two ways such as encoding and data hiding (Liu and Ke 2018). A mix of these two strategies can be utilized to build information security (Karolin and Meyyapan 2015). However, security can be approached from various perspectives like password, confirmation, distinguishing proof (Singh et al. 2018), watermarking systems (Thakur et al. 2018b; Kumar et al. 2018a, b) and so on (Nagdive and Raut 2015). In such a manner, diverse image cryptosystems were prescribed earlier in light of the fact that encryption is seen as an effective and direct strategy to secure private information (Linju and Mathews 2016). Encryption and decryption of the information are observed as the perfect ways to ensure the data is secure and respected. Share period for the visual cryptography ought to be in the manner such that it can conceived through watermarking using some watermarking procedures. One can use these watermarked offers for recuperating the covered information (Singh et al. 2016).

✉ Mohamed Elhoseny
mohamed_elhoseny@mans.edu.eg

K. Shankar
shankar.k@klu.ac.in

R. Satheesh Kumar
satheeshpkd@gmail.com

S. K. Lakshmanaprabu
prabusk.leo@gmail.com

Xiaohui Yuan
xiaohui.yuan@unt.edu

[1] School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India

[2] Faculty of Computers and Information, Mansoura University, Mansoura, Egypt

[3] Department of Computer Science and Engineering, Sahrdaya College of Engineering and Technology, Kodakara, Kerela, India

[4] Department of Electronics and Instrumentation Engineering, B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

[5] Department of Computer Science and Engineering, University of North Texas, Denton, USA

Published online: 10 December 2018

The share-based image has more noteworthy favorable positions over customary steganography method. The quality of security is an increment in spite of geometrical and some other gatecrasher-based assaults (Shankar and Eswaran 2017; Vengadapurvaja et al. 2017). The procedure of share-age utilized 'image pixel extension' method for cryptography reason (Younes 2016). Shares independently uncover no data, about the (Zhang et al. 2017) first secret image, other than its measure and transmit these shares to a number of members. The secret can be recuperated by superimposing edge number of shares with no mind-boggling calculation (Baghel and Goyal 2016; Shankar and Eswaran 2016a, b, c). This effort can result in noteworthy shares rather than a couple of shares without any information. In the current study, water making-based (Dharwadkar and Amberker 2010) idea is used for visual cryptography.

The watermarking procedure produces a surface-based share and encrypts the image (Mishra and Sharma 2014; Srivastava et al. 2018). The wavelet transforms' work utilized 2D change for the extraction of the feature for the age of key utilized shading model (Revathy 2014). Wavelet is nothing but a waveform of the adequately-restricted term that has normal estimation of zero (Zhang et al. 2017). The term wavelet originates from the way how it incorporates zero; it waves here and there over the pivot (Nazimul and Choubey 2015). Wavelets change over into a progression of wavelets in the image that can be sidelined more effectively than pixel squares. It has harsh edges and can render images better by eliminating the obscurity (Dipalee and Siddhartha 2015). Homomorphic cryptosystems are uncommon cryptosystems with the capacity of performing expansion and augmentation tasks (Zhang and Xu 2018) using scrambled information without uncovering any data about unique information (Pang 2009). Homomorphicencryption can be utilized as a part of request to shield the common images from block attempt in the presence of transmission &capacity in addition to combining the encoded images to frame another image so as to decrease the transfer speed use (Vengadapurvaja et al. 2017). In addition, because of the clamor's expansion proportionate to the quantity of encryption to acknowledge the homomorphic tasks completely (Dasgupta and Pal 2016) and to do the homomorphic activities boundlessly, Gentry came up with the concept of encryption (Kuppusamy and Thamodaran 2013; Shankar and Eswaran 2015a, b, c). The utilization of the normal dialect-writing computer programs are considered here. Genetic Algorithm (GA) is the best optimization heuristics procedure (Noura Metawaa et al. 2017) to reduce the ideal opportunity for key (Dardzinska 2007) look and computational many-sided quality while breaking any sort of the figure. Among the manmade brainpower algorithms, Genetic Algorithm, tabu hunt, PSO, HS are utilized for different applications.

The second section conducted an audit of literature regarding image security and under second 3, the motivation of the proposed modeling is presented. At that point segment, 4th section examines the proposed technique while the fifth segment discusses the simulation result analysis concluded with the future work of this paper.

2 Literature survey

In 2016 (Talarposhti and Jamei 2016), recommended the most extreme entropy and least correlation coefficient that can be acquired by applying a harmony search calculation in it. This procedure is segregated into two steps. In the initial step, the dissemination of a plain image, utilizing DHS to augment the entropy as a wellness capacity, was performed. Further, in the second step, a flat and vertical stage was connected to the best cipher image, which is acquired in the past advance. Furthermore, DHS has been utilized to limit the correlation coefficient as a wellness work in the second step. From the results, it was demonstrated that by utilizing the proposed technique, the most extreme entropy and the base correlation coefficient can be acquired for which the values are 7.9998 and 0.0001 approximately.

A study was conducted by Houssein et al. (2016) regarding the Advanced Encryption System (AES) and concealing the information utilizing Haar Discreet Wavelet Transform (HDWT). HDWT was planned to diminish the many-sided quality in image steganology, while giving less image mutilation and lesser perceptibility. One-fourth of the image conveyed the points of interest in a image at locale whereas other three districts conveyed a less subtle elements of the image. Then the ciphertext is hidden at any Least Significant Bits (LSB) positions in the less-itemized areas of the bearer image and if in case, if the message doesn't fit well in the principal LSB, the second LSB is utilized instead of it.

The rule of secure multi-party calculation for the security of votes (Sanyasi Naidu et al. 2016). Secure multi-party calculation enables multiple gatherings to take an interest in a calculation. Security, accuracy dependability and straightforwardness are the significant worries in these systems. The voters, who cast multiple votes amid the voting procedure, are guaranteed to be forestalled by biometric distinguishing proof of the votes which could be utilized for making their choice and confining them to cast their votes only once.

Challa et al. (2015) proposed down-to-earth usage of image handling activities on encrypted images which are put away in cloud or transmitted over an unsecured channel, utilizing (Learning with Errors) LWE-based homomorphic encryption scheme. LWE scheme turned out to be an incredibly flexible, secured and well reasonable for homomorphic encryption. LWE-based homomorphic encryption is actualized to investigate the tasks on encrypted paired/dark scale image. Likewise, the issues emerge when there is a prerequisite for openly sharing and registering private information.

Banik et al. (2015) proposed new method of image steganography that utilized Lorenz Chaotic Encryption to encode the mystery message, 3-level DWT to cover up encrypted information and visual cryptography to share stego image in a mystery correspondence.

Elliptic Curve Cryptography (ECC) method has turned out to be a compelling cryptographic method (Toughi et al. 2017). The elliptic curve random generator was characterized by National Institute of Standards and Technology (NIST), to produce a grouping of discretionary numbers, in light of curves. The random age stage depends on openly-shared key and a changing point G, which is the generator of a curve to get random arrangements. At that point, AES is connected to these arrangements, securing self-assertive keys for encrypting image. AES nearby all-around disseminated random gives a conspicuous encryption method.

Elhoseny et al. (2016b) proposed another image steganography approach for securing medical information. Swapped Huffman tree coding is utilized to apply lossless pressure and complex encryption to the payload before inserting into the cover image. Furthermore, 'just-edge districts' of the cover image are utilized to implant the mystery information which offers high intangibility. The outcomes demonstrated that the proposed technique guarantees classification and mystery of patient data while looking after indistinctness.

Shankar and Lakshmanaprabu (2018) the proposed the Homomorphic encryption with Ant Lion Optimization (ALO). For improving the security level, an algorithm called ALO is introduced. Based on this ALO, the best-encrypted image is illustrated as in the view of maximum entropy. Sokouti et al. (2016) have proposed the Goldreich Goldwasser Halevi (GGH) algorithm, In addition to this, the GGH algorithm does not enhance the size of the image and finally, the difficulty will remain the system. One drawback is there, that is the Chosen Cipher Text Attack for prove effectiveness of work. Kumari et al. (2018) Have analyzed a solid verification conspire assumes a pivotal role in shielding communications over the Internet. The proposed ECC scheme is powerless to the client and server impersonation attacks. Likewise, their plan neglects to accomplish client secrecy and shared authentication. Many image encryption procedures are proposed to ensure confidentiality of information. The proposed method must consider these constraints. Be that as it may, the greater part of the proposed methods are not applicable for advanced image because of image structure and estimate; in this manner, the customary cryptosystems cannot be connected on WSN by Shaheen et al. (2018). The arrangement of telecare medical data framework over open systems offers ascend to the risk of uncovering threat medicinal data to illicit elements. An enhanced 3FA plan and demonstrate that the new plan satisfies session key mystery and shared confirmation utilizing the formal check tool verification (Jiang et al. 2018).

3 Issues in current system

The secret image is exchanged between the sender and the recipient and the secret image is delegated shares (Shankar and Eswaran 2016a). Every share contains a piece of secret image data (Shankar and Eswaran 2017). There are different cases in which the procedure utilized may not be exceptionally effective i.e., the first image and the subsequent image can be recognized by exposed human eyes itself. There are a few security issues related to advanced image preparing and transmission due to which it is important to keep up the uprightness and the privacy of the image. Optimization systems and chaotic elements of the security procedure (Thakur et al. 2018a) are intended to expand entropy and the most-reduced coefficient for images. These utilize a similar key for encryption and decryption making it simple for the gatecrasher to get access to the data. At this point, the cipher content is developed; it must be unscrambled into unique plain content with no misfortune. Despite that, the cipher images might be unscrambled to plain images in some misfortune ways since image measured is substantially bigger than the instant message. So conventional cryptosystems require much time to encode the image information specifically (Elhoseny et al. 2016a, b, 2017). The Internet due to which there is a need to guarantee data security and wellbeing to safeguard against unapproved get to.

4 Methodology

'Visual secret share creation' process allows the visual data to be encoded such that the decryption can be performed by human visual system. Our proposed methodology analyzes the image security process using wavelet transform based secret share creation process. Initially, the secret image is separated into the corresponding RGB color channels then DWT is considered to generate sub bands with the combination of low and high bands of RGB. Once the sub bands are generated, the secret sharing scheme is utilized to generate the multiple shadows of the secret image.

The Homomorphic Encryption (HE) algorithm is applied to encrypt the multiple shadows for increasing the shadows security. Here the HE key values are optimized using Opposition based Harmony Search (OHS) optimization algorithm to achieve the high reconstructed image quality. The quality of the image is taken as fitness value for the optimization process such as PSNR value is considered. After choosing the optimal keys, the images are encrypted to maximizing security level. Figure 1 shows the block diagram of the proposed scheme.

4.1 Secret images with conversion

Color secret images can be shared via circular segments to build color cryptography. The pixel estimations of the secret color image were expelled and took as RGB pixel esteems and these characteristics freely appeared as a framework for the span of the network. The conversion depended on color image submitted alongside the info gray image (Reddy and Meenakshi 2014). A grayscale image is extremely constrained in its ability to shroud a secret image. By and by, every pixel of a color image comprises three channels (RGB) and every channel has 8 bits, i.e. every pixel has 24 bits. The first secret images to gray conversion is arrived at through the condition (1).

$$\text{Gray\_Image} = \left[\frac{(R_p + G_p + B_p)}{3} \right] \quad (1)$$

Grayscale images are set as the secret images or the classified messages. In the above condition R_p, G_p, B_p are pixel estimations of each band in color images. Every pixel from the secret image is encoded into numerous subpixels, in each shadow image utilizing a framework to decide the color of the pixels. The gray qualities in images are in the vicinity of 0 and 255 and so the variable estimation of the prime number ‘P’ utilized, is the nearest prime number of the most extreme estimation of the gray level for secret image.

4.2 Wavelet-based visual secret share (VSS) creation

VSS is one of the proficient techniques for concealing a image. It is performed by isolating the image into different negligible shadows. These individual shadows do not uncover anything about the mystery, other than its size. Our method, consider innovative idea to create and hiding the shares of gray images using DWT sub bands, here consider the coefficients as haar wavelets. Shadow recovery process incorporates removing shadows from cover images and afterward recovers the mystery by covering shadows. From DWT sub-band mystery (Dayanand et al. 2014), visual shadows are made. The generation of shadows occurrence value of detail component is discussed. The level of shadow makes some portion of transform function and the itemized clarification of shadow creation talked about in underneath area.

4.2.1 Discrete wavelet transform

Discrete wavelet decomposition of an image delivers multi-determined portrayal of the image. A multi-determination portrayal gives a basic as well as various leveled system to translate the image data. It is computationally difficult to dissect aimage using all wavelet coefficients due to which one may think about whether it is adequate to pick a discrete subset of the upper half plane, to have the capacity and to recreate a signal from the relating wavelet coefficients. The image is spoken by two-dimensional signal functions where the wavelet transform disintegrates the image into four recurrence groups, to be specific such as LL, LH, HL,and HL (L—Low and H—High) subgroups. If comprises of decomposition and recreation channels with wavelet coefficient as haar wavelets. The point-by-point images, LH, HL, and HH contains high recurrence segments as shown in Fig. 2. To

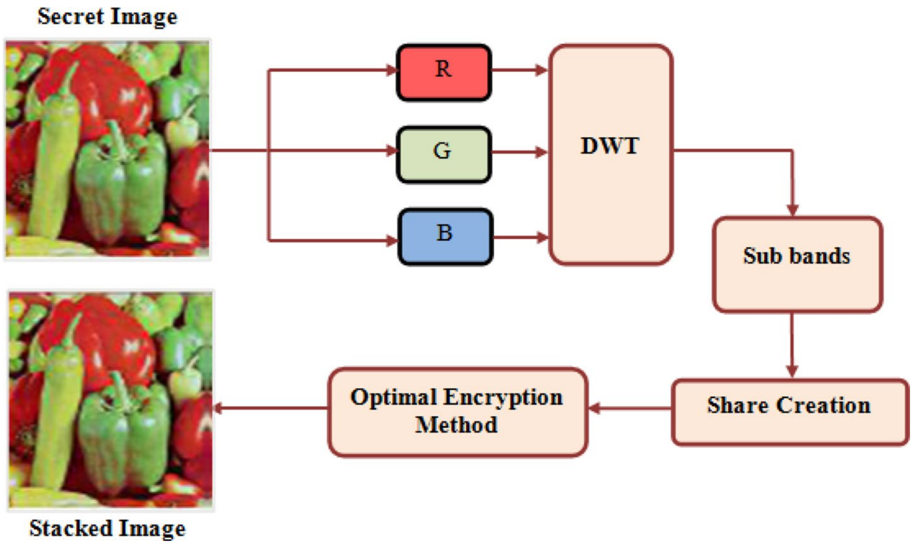


Fig. 1 Graphical representation of the proposed model

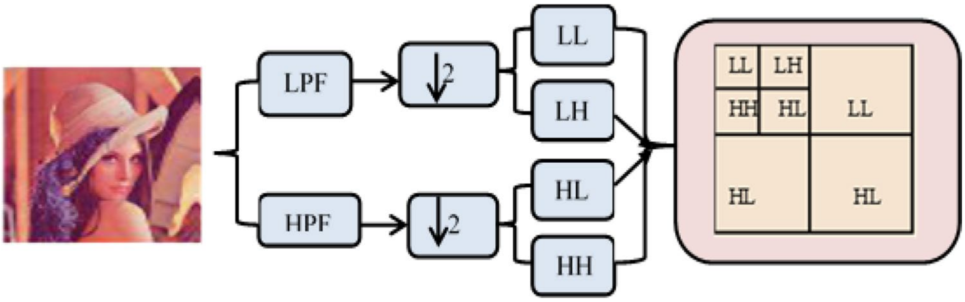


Fig. 2 Wavelet subbands

acquire the following courselevel of wavelet coefficients, the subband LL alone is additionally disintegrated and fundamentally examined.

4.2.1.1 Haar wavelet coefficient Haar wavelet is the most straightforward kind of wavelet. In discrete frame, Haar wavelets are identified with a numerical task called Haar transform. The Haar transform fills in as a model for all other wavelet transforms. Like all wavelet transforms, the transform decays a discrete image into two sub-images of half its length. Haar's wavelet function can be shows as equation as follows.

$$V(t) = \sum_{i\in m}\sum_{j\in n}(v, H_{m,n}) * H_{m,n}(t) \tag{2}$$

$$H_{m,n}(t) = \begin{cases} 1 & 0 \le t \le 1/2 \\ 1 & 1/2 \le t \le 1 \\ 0 & \text{Otherwise} \end{cases} \tag{3}$$

One sub-image is a running normal or pattern; the other sub-image is a running contrast or vacillation. Wavelets change over the image into a progression of wavelets that can be put away more effectively than pixel squares. Consequently, N-level decomposition will finally have $3n + 1$ differing recurrence groups, which fuse with high recurrence groups but only one LL recurrence band.

4.3 Visual secret share creation

In this shadow creation procedure, a binary secret image is encoded into 'n' shadows from the wavelet subbands as shown in the Fig. 3 (Dayanand et al. 2014). Every last shadow comprises both black and white pixels in the state of clamor and are especially large in measurement when compared to that of the secret image. Every last original pixel of the secret image emerges, in 'n' adjusted versions, is labeled as 'shadows'. Every last shadow, thus, is a gathering of sub-pixels of the RGB image. The shadow for RGB is separately shown as

$$R_p = \int_1^k \lim_{k\to 1,\text{to.no.of.pixel}} R_{mn-\text{Subband}} \tag{4}$$

$$G_p = \int_1^k \lim_{k\to 1,\text{to.no.of.pixel}} G_{mn-\text{Subband}} \tag{5}$$

$$B_p = \int_1^k \lim_{k\to 1,\text{to.no.of.pixel}} B_{mn-\text{Subband}} \tag{6}$$

In the above conditions, the position of a matrix of each band and k total number of pixels are shown. The R, G and B band pixel values are extracted from the original image and are taken as the separation matrix. Finally, two shadow images are obtained using shadow creation conditions in

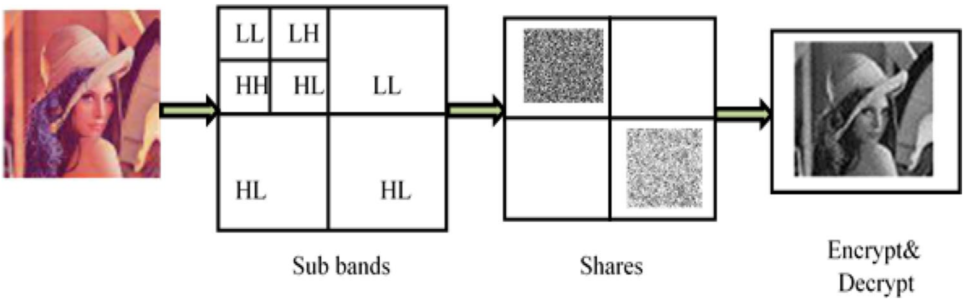


Fig. 3 Wavelet-based share creation process

this investigation; an inventive visual secret share generation procedure is a utilized process used to produce two shadows for every one of the image. These individual shadows don't reveal anything about the secret, other than its size. The original secret can be reconstructed by combining every one of the shadows. In the encryption process, every secret pixel is turned into two shadows, and each shadow belongs to the corresponding shadow image.

4.3.1 Steps involved in DWT-based VSS model

1. Select the input secret image with redress width and tallness which spreads from RGB to grayscale image.
2. Apply wavelet transform on luminance part to produce four sub-bandssuch as LL, HH, LH, and HL and it is identified with low pass, high pass, vertical and flat measurements.
3. In light of these sub-bands, make two lattice for offers of a white mystery pixel to be the same while those of a black mystery pixel.
4. Replace the sub-bandsby the offer. Keeping in mind the end goal to perform supplant task, the span of offer ought to be equivalent to size of the subbands. In this way, single offer is encoded three times in cover image.
5. A reverse DWT is conveyed to recompose the image
6. Initialize variable text style shading and record value

Visual secret sharing is a productive strategy for hiding an image. It is finished by dividing the image into various meaningless shadows. These individual shadows do not reveal anything about the secret, other than its size and transmit these shadows to a number of participants. The secret can be recovered by superimposing a threshold number of shadows with no unpredictable calculation.

4.4 Encryption modeling

Encryption is the way toward clouding data to make it mixed up without unique information. It has been utilized to secure interchanges for quite a long time, however, just associations and people with an unprecedented requirement for mystery had utilized it. Each encryption and the unscrambling process has two perspectives: the calculation and the key used for the encryption and decoding. In their procedure, initially, various encoded images are developed utilizing the original image with the assistance of the optimization work.

4.4.1 Homomorphic encryption

Homomorphic encryption enables the calculation to be done on cipher image and afterward, the consequences of the activities performed can be unscrambled by the proprietor. Presently the information proprietor can get an indistinguishable message from the event that it is performed on two plain images. A proficient encryption calculation, which fulfills the homomorphic property to perform encryption and decoding on images, is proposed. For picking optimal keys (Private and Public keys) in HE (Elhoseny et al. 2016a, b), the help of optimization display is required (Shankar and Eswaran 2016b). This procedure has some default steps as follows.

4.4.2 Oppositional harmony search (OHS) optimization for key generation

A strategy is designed for encoding and translating the keys and related image using a symmetric key; both mystery and reliability security is provided. A private key and its relating public key; a key match is used with an asymmetric key (public-key) calculation. HS was inducted by the act of spontaneity of Jazz musicians. The musicians quickly refined their individual impromptu creation by bringing a tasteful amicability. In order to enhance this execution, the current study has considered an oppositional process with them and this graphical model is illustrated in the Fig. 4.

It is characterized as follows

$$O_j^* = L_j + H_j - O_j \tag{7}$$

On the off chance, O is a solution in existing search space and when $O_j^* \in [L_j, H_j]$, then according to opposition-based learning model, a new solution O_j^* in the transformed space is shown in the above equation. By and large, HS technique contains some vital terms such as

HMS Harmony memory size, it is the number of solution vectors in the harmony memory

HMCR Harmony memory considering rate, the range starts from ∈ [0, 1]

PAR Pitch adjusting rate ∈ [0, 1]

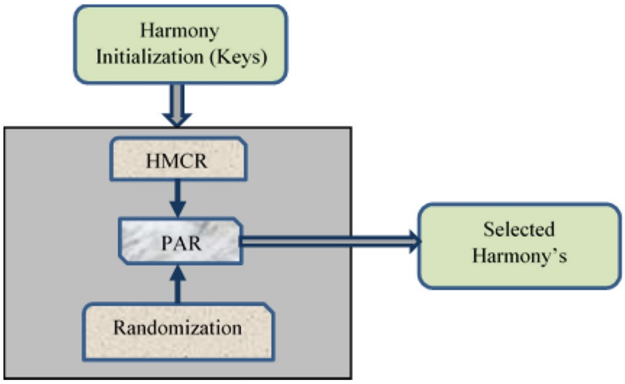


Fig. 4 Process for HS optimization

4.4.2.1 Initialization process This initialization of prime numbers is considered to produce new key size for the optimal key selection process.

$$\text{Key}_{1,2\ldots n} = \{k_1, k_2, \ldots k_n\}$$

4.4.2.2 The objective function for key optimization PSNR is an articulation, for the proportion between the most extreme conceivable estimation of a signal and the energy of mutilating clamor, which influences the nature of its portrayal. The original image and the reference image must be of a similar size and class.

$$\text{Fitness} = \text{Max (PSNR)} \tag{8}$$

$$PSNR = \frac{1}{s}\sum_{i=1}^{\text{shares}} 10\,\log_{10}\left(255^2/_{MSE}\right) \tag{9}$$

This PSNR condition 's' as number DWT applied shadows. In PSNR, the square of the peak value in the image is to be taken (in case of an 8-bit image, the peak value is 255) and divided by mean square error.

4.4.2.3 Improvised new harmony for key generations A New Harmony vector is created based on three standards like memory thought, pitch modification and irregular determination. The process of creating a novel harmony is known as impromptu creation. HM is equivalent to the phase where the artist uses memory to deliver a tune. The estimations of the other choice factors are chosen comparatively. The HMCR is the rate of choosing one incentive from the authentic qualities stowed in HM, while it is also the rate of erratically picking one incentive from the possible scope of qualities.

$$P_i' = \left\{P_i \in \begin{Bmatrix} P_i^1, P_i^2, \ldots P_i^{\text{HMS}} \text{ with Probaility } HMCR \\ P_i' \in P \text{ with Proability } (1 - HMCR) \end{Bmatrix}\right. \tag{10}$$

For example, an HMCR of 0.90 is assigned that the HS calculation will choose the choice variable incentive for most of the part put away qualities in the HM with 90% probability.

4.4.2.4 Pitch adjustment 'Every component obtained by the memory consideration is examined to determine whether it should be pitch-adjusted. This operation utilizes the PAR $\in [0, 1]$ parameter that is the rate of pitch adjustment as follows':

$$PAR = \begin{cases} \text{Adjusting pitch with Proability} \\ 0 \text{ Proability } (1 - \text{pitch}) \end{cases} \tag{11}$$

On the other hand, a very high pitch-adjusting rate with a wide bandwidth may cause the solution to scatter around some potential optima as in a random search.

4.4.2.5 Update harmony memory For each new estimate of harmony, the estimation of target work was figured. In the off chance, New Harmony vector is superior to the most exceedingly-terrible harmony in the HM whereas the New Harmony is incorporated into the HM and the current most exceedingly-terrible harmony is barred from HM. Despite the fact that changing pitch has a comparative part, it seems to be constrained for certain nearby pitch alteration which consequently corresponds to a local search.

4.4.2.6 Stopping process The best solutions which achieve the objective function are discovered and the algorithm is prepared to give exact solutions in light of maximizing the objective function. Until getting the optimal key the process will be repeated.

4.5 Optimal private and public keys

According to the processes mentioned earlier, the new arrangements sets are achieved. At that point, the wellness esteem is discovered for the new arrangements. The optimal public key is that the one which can easily be used to scramble yet cannot be utilized to decrypt messages. The private key is the simple backpack, which gives a basic mode to decrypt the message (Shankar and Eswaran 2016c).

4.6 Shadows encryption and decryption process

Encryption appears as a decent method to secure and protect the outsourced applications, particularly when taking care of whole amount of information written. The utilization of bearer image for image encryption has been introduced in literature (Younes 2016) utilizing optimal private key cryptosystem in recurrence area. In any case, by encoding every pixel independently utilizing homomorphic encryption, the administration can work on by utilizing the encrypted pixels. At that point, the administration can process the encrypted image without decoding. In the decoding technique, the image figure is to be audited which includes encrypted pixel-addressed purchase and the secret vector.

$$\text{Encryption}: O_{\text{privateKey}} = (k, i) \tag{12}$$

Cipher image to Decrypt process Cipher image to Decrypt Process: Cipher $\in E*_{k^2}$

$$\text{Decryption}: \frac{D(\text{cipher}^{\alpha} \bmod k^2)}{D(i^{\alpha} \bmod k^2)} \bmod k \tag{13}$$

The decryption procedure is incorporated using two cloaks, specifically, the mystery cover and the even masks in a relentless movement. Decoding of the image, along these lines, includes the application of unscrambling system for each encrypted estimation of the pixel in the encrypted image. In the setting, where bland encryption conspire is

Table 1 Results ofthe proposed image security model for Lena

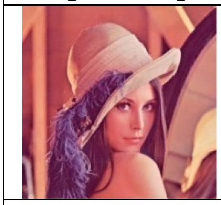
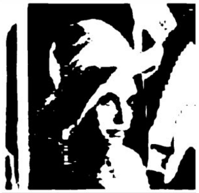
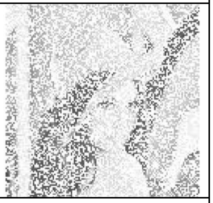
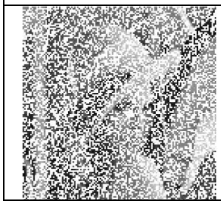
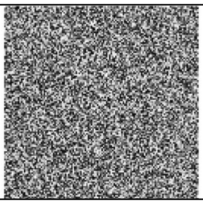
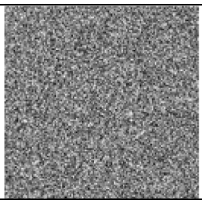
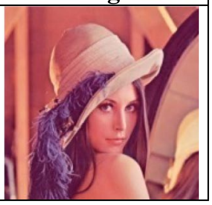
Original Image	Grayscale Image	DWT	Shadow1
			
Shadow2	Encrypted Shadow1	Encrypted Shadow2	Final Decrypted Image
			

Table 2 Results of proposed image security model for house

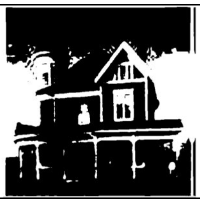
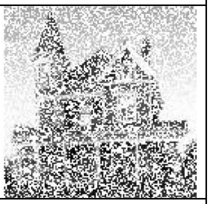
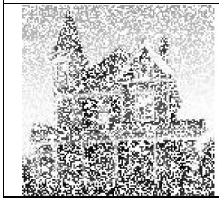
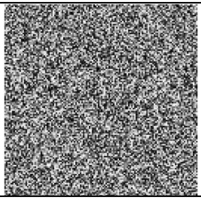
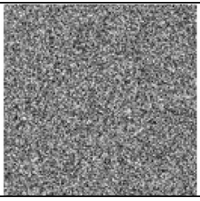
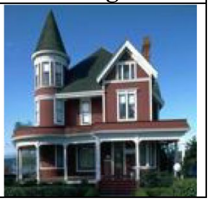
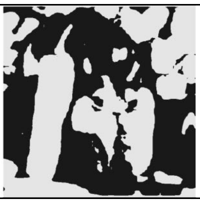
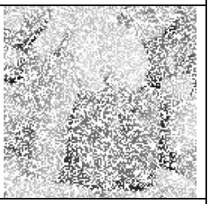
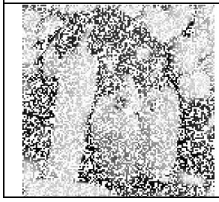
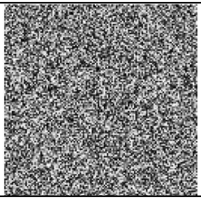
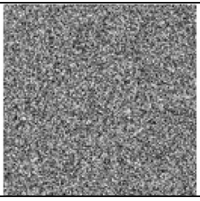
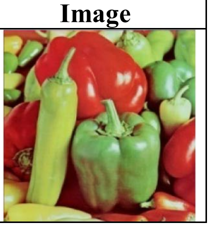
Original Image	Grayscale Image	DWT	Shadow1
			
Shadow2	Encrypted Shadow1	Encrypted Shadow2	Final Decrypted Image
			

Table 3 Results of proposed image security model for peppers

Original Image	Grayscale Image	DWT	Shadow1
			
Shadow2	Encrypted Shadow1	Encrypted Shadow2	Final Decrypted Image
			

utilized, all the activities associated with image handling are perhaps just on the unencrypted image.

4.7 Reconstruction process

All the decrypted shadows are stacked (shadow 1 and shadow 2) together to recover the mystery image. Just if every one of the quantities of mystery shared images is stacked together, it is conceivable to uncover the insider facts.

$$\mathrm{Re}_{\mathrm{Im}\,age} = \{R_{p(sh1,sh2)} + G_{p(sh1,sh2)} + P_{p(sh1,sh2)}\} \tag{14}$$

On the off chance that the offer images are harmed amid transmission or generation, the aftereffects of the stacked mystery are likewise to be influenced. In the private image, each offer is part of block image and the prime number is chosen alongside the optimal key values.

Table 4 Results of proposed image security model for baboon

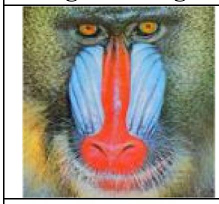
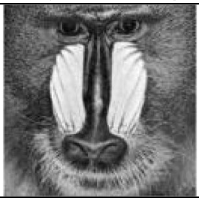
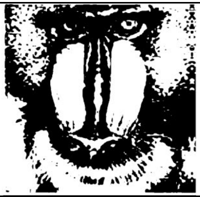
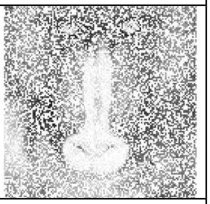
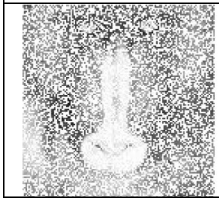
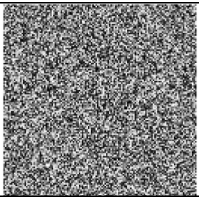
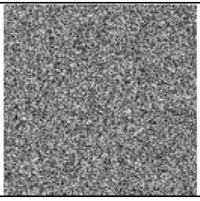
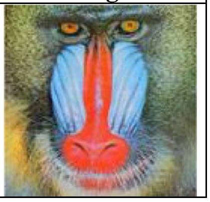
Original Image	Grayscale Image	DWT	Shadow1
			
Shadow2	**Encrypted Shadow1**	**Encrypted Shadow2**	**Final Decrypted Image**
			

Table 5 Performance analysis of the proposed scheme

Images	PSNR	Entropy	MSE	MAE	CC
	52.21	7.69	0.28	0.36	0.99
	51.2	7.05	0.21	0.3	0.85
	48.85	7.88	0.19	0.32	0.92
	52.2	7.68	0.25	0.42	0.93
	51.89	7.55	0.25	0.45	0.97

5 Result and analysis

‘The proposed DWT-based image security process was implemented in MATLAB 2016 with a system configuration of i5 processors with 4 GB RAM. In this paper, the proposed model results are compared with existing papers and general optimization techniques. This analysis model considers some standard images like Lena, baboon, house, Barbara, and pepper images and for this purpose, performance metrics such as Entropy, PSNR, Mean Absolute Error (MAE), Mean Square Error (MSE) and Correlation Coefficient (CC) measures were considered.

Tables 1, 2, 3, 4 and 5 demonstrates the proposed DWT-based offer made encryption framework. At first, the image got changed over into RGB to dark those DWT after which the offers are made. In secret image, RGB band was created and each band had two offers which are independently scrambled and decoded. Security examination covers histogram investigation, correlation investigation, and entropy examination. This investigation covers most extreme PSNR value to be 53.42 dB in images after unscrambled part correspondingly in other image exhibitions. At whatever point, the correlation value is little and this implies that the encryption procedure accomplished high haphazardness between the adjacent pixels in the scrambled image in CC. The numbers demonstrate that the image has better execution with respect to time since it is less in pieces. But the PSNR indicated that more grounded figuring in primate image twosome to a bigger number of squares which prompt increment in a number of chains longer secret key that accomplishes elite insecurity.

Figures 5 and 6 demonstrate the comparative examination of PSNR and entropy of the proposed security display with other systems like HE, HE with congruity pursuit, HE with Ant Lion Optimization (ALO) (Shankar and Lakshmanaprabu 2018) and ECC methods. When using the proposed calculation, the client required not to preprocess the image that corrupts the visual quality. The stacked image from the

Fig. 5 Comparative analysis for PSNR

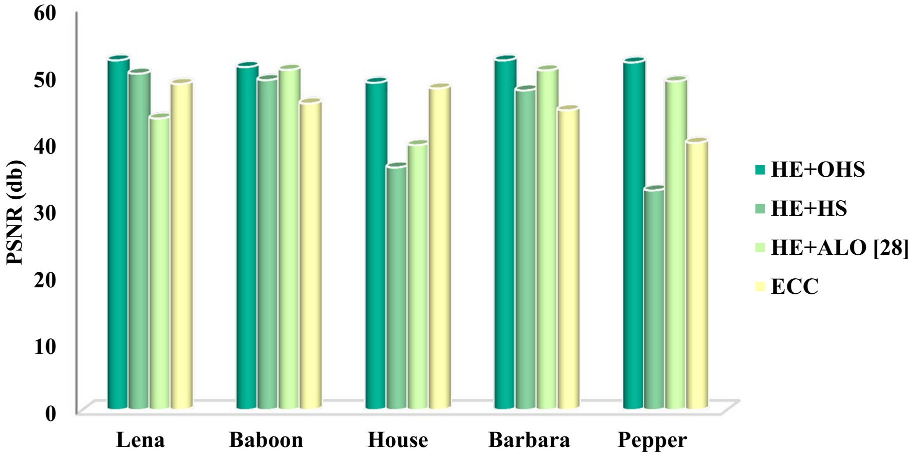
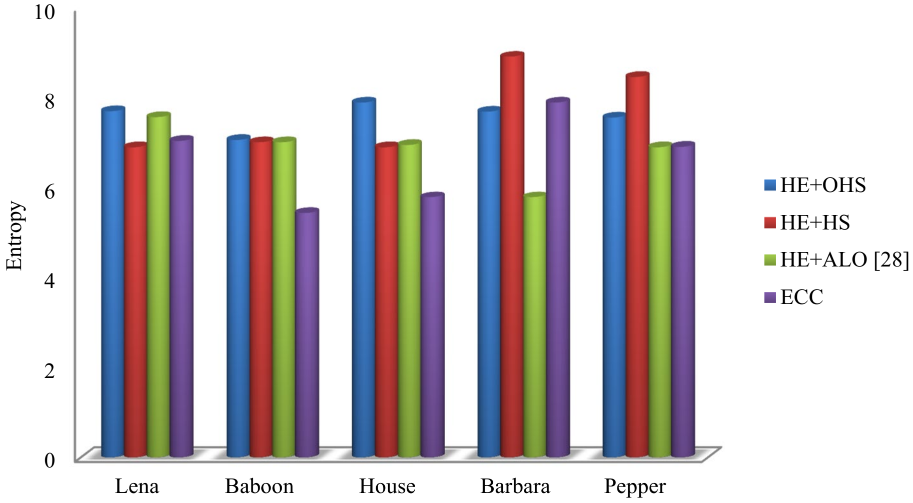


Fig. 6 Comparative analysis for entropy



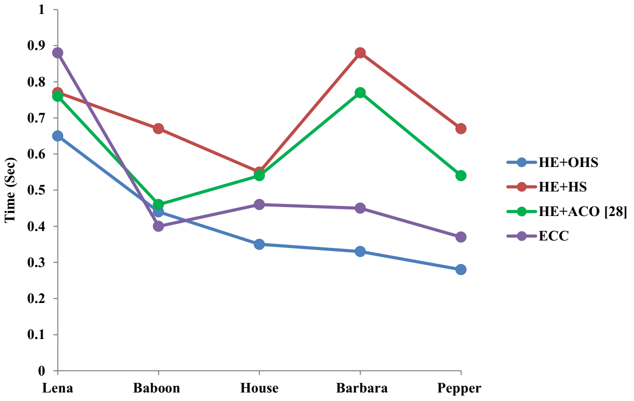


Fig. 7 Encryption time analysis

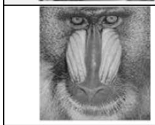
current proposed strategy is clear and the visual quality is subsequently improved with most extreme PSNR rate for all images. On the off chance that utilization improvement process in encryption method, a few immense time was taken for scrambling and unscrambling process thought it is exceptionally secure. Figure 6 entropy shows that if the yield of such a discharges images with entropy. In baboon image ECC produce minimum entropy, the reason is pixel value and keys of encryption; there exists a certain level of consistency, which debilitates its security. The results likewise demonstrated that expanding the number of pieces by utilizing smaller square sizes brought about a lower correlation and higher entropy.

Figure 7, for a time, expected to finish the encryption stage is one of the normal factors that is utilized to assess the execution of the encryption procedure. A decent image encryption system is the one that directs its encryption tasks in a brief span. The current proposed show just sets aside more opportunity for the examination within 0.88 s when compared to others.

Table 6 demonstrates the attack-connected outcomes for the proposed display. In this, the execution measures like PSNR and entropy get most extreme value attack process. Absolutely the distinction between the two processes ranged from 45.78 to 52.2%. This plan gives greater security to secret offers that are strong against a number of attacks. The data spillage in the encryption process is immaterial and the encryption framework is secure upon the entropy attack.

The comparison of 'with attack' and 'without attack' is illustrated in the Fig. 8. Image encryption system is the one that creates a high proportion of clamor in the encoded image with low PSNR value. These two processes are the most extreme PSNR accomplished in 'without attack connected images' compared to other ones. Essentially Entropy is processed from the chosen hinder in the image whose size depends on the image measure. Whatever left of pieces are chosen, they have an indistinguishable entropy from applicants that are utilized for producing sufficient and substantial secret-key space to encode the image later.

Table 6 Attack-based results

Grayscale	Decrypted	PSNR	Entropy	MSE	MAE	CC
		50.22	6.45	0.56	0.66	0.82
		25.22	5.89	0.78	0.82	0.83
		36.2	5.6	0.45	0.55	0.74
		45.22	10.2	0.65	0.69	0.76
		46.52	9.56	0.74	0.79	0.66

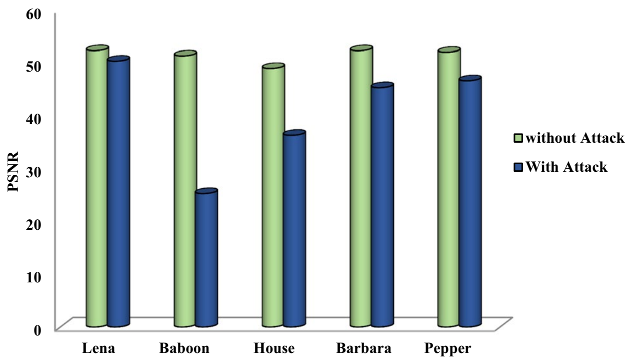


Fig. 8 With attack vs without attack

6 Conclusion

The current study considered and analyzed the image security investigation with DWT-based sharer creation process. The results reveal that the proposed scheme ensures best reconstruction of images with desirable quality due to the tunable feature in the secret shadows. Security purpose optimal key based HE technique with PSNR as fitness consider, it's more efficient compared to other security techniques. From the optimal public-key is increased security: the private keys do not ever need to be transmitted images. From the implementation results the maximum PSNR in HE-OHS is 58.46 dB of encrypted and decrypted image. The secret key values may be different from one image to another which adds more ambiguity at the side of attackers about the key itself. In future work, we will have considered medical, identity images to enhance the security level with help of innovative swarm optimization in frame work.

References

Baghel SS, Goyal A (2016) Improved the security strength of visual cryptography using feature-based watermarking technique. Int J Comput Appl 153(11):9–13

Banik BG, Bandyopadhyay SK (2015) Secret sharing using 3 level DWT method of image steganography based on Lorenz chaotic encryption and visual cryptography. In: Computational Intelligence and Communication Networks (CICN), 2015 International Conference on IEEE, pp 1147–1152

Challa R, Vijayakumar G, Sunny B (2015). Secure image processing using LWE based homomorphic encryption. In: Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on IEEE, pp 1–6

Dardzinska-Glebocka A (2007) Optimization algorithm and data security problem in distributed information systems. In: Signal-image technologies and internet-based system, 2007. SITIS'07. Third International IEEE Conference on IEEE, pp 116–120

Dasgupta S, Pal SK (2016) Design of a polynomial ring based symmetric homomorphic encryption scheme. Perspect Sci 8:692–695

Dayanand IE, Kumar RS (2014) Analysis of secret image sharing using shared image. Int J Comput Appl 108(7):35–39

Dharwadkar NV, Amberker BB (2010) Watermarking scheme for color images using wavelet transform based texture properties and secret sharing. Int J Signal Process 6(2):93–100

Elhoseny M, Yuan X, ElMinir HK, Riad AM (2016a) An energy efficient encryption method for secure dynamic WSN. Secur Commun Netw 9(13):2024–2031

Elhoseny M, Elminir H, Riad A, Yuan X (2016b) A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. J King Saud Univ Comput Inf Sci 28(3):262–275. https://doi.org/10.1016/j.jksuci.2015.11.001

Elhoseny M, Hosny A, Hassanien AE, Muhammad K, AK Sangaiah (2017) Secure automated forensic investigation for sustainable critical infrastructures compliant with green computing requirements. IEEE Trans Sustain Comput:. https://doi.org/10.1109/TSUSC.2017.2782737

Gupta D, Choubey S (2015) The discrete wavelet transforms for image processing. Int J Emerg Technol Adv Eng 4(3):598–602

Houssein EH, Ali MA, Hassanien AE (2016) An image steganography algorithm using haar discrete wavelet transform with advanced encryption system. In: Computer Science and Information Systems (FedCSIS), 2016 Federated Conference on IEEE, pp 641–644

Jiang Q, Chen Z, Li B, Shen J, Yang L, Ma J (2018) Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. J Ambient Intell Humaniz Comput 9(4):1061–1073. https://doi.org/10.1007/s12652-017-0516-2

Karolin M, Meyyapan DT (2015) RGB based secret sharing scheme in color visual cryptography. Int J Adv Res Comput Commun Eng 4(7):151–155

Kumar C, Singh AK, Kumar P (2018a) Improved wavelet-based image watermarking through SPIHT. Multimed Tools Appl:. https://doi.org/10.1007/s11042-018-6177-0

Kumar C, Singh AK, Kumar P, Singh R, Singh S 2018b SPIHT-based multiple image watermarking in NSCT domain. Concurr Comput Pract Exp. https://doi.org/10.1002/cpe.4912

Kumari S, Karuppiah M, Das AK, Li X, Wu F, Gupta V (2018) Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography. J Ambient Intell Humaniz Comput 9(3):643–653. https://doi.org/10.1007/s12652-017-0460-1

Kuppusamy K, Thamodaran K (2013) Optimized hybrid security mechanism for image authentication and secrecy using PSO. Int J Netw Secur Appl 5(5):115–128

Linju PS, Mathews S (2016) An efficient interception mechanism against cheating in visual cryptography with non pixel expansion of images. Int J Sci Technol Res 5(01):102–106

Liu J, Ke L (2018) New efficient identity based encryption without pairings. J Ambient Intell Humaniz Comput.. https://doi.org/10.1007/s12652-018-0756-9

Mishra DC, Sharma RK (2014) Application of algebra and discrete wavelet transform in two-dimensional data (RGB-images) security. Int J Wavelets Multiresolut Inf Process 12(06):1450040–1450041

Nagdive MPS, Raut AB (2015) Image visual cryptography by using haar wavelet-based decomposition. Int J Adv Res Comput Eng Technol 4(4):1261–1265

Nazimul Islam Gupta D, Choubey S (2015) Security improvement of image by visual cryptography using super imposed wavelet transform in image processing. Int J Adv Res Comput Sci Softw Eng 5(5):498–503

NouraMetawaa M, KabirHassana, Elhoseny M (2017) Genetic algorithm based model for optimizing bank lending decisions. Expert Syst Appl 80:75–82

Pang CJ (2009) An image encryption algorithm based on discrete wavelet transform and two dimension cat mapping. In: Networks security, wireless communications and trusted computing, 2009. NSWCTC'09. International Conference on (Vol 2, pp 711–714). IEEE

Rani MMS, Mary GG (2016) Enhancement of RGB shares of visual cryptography using PSO. Int J Comput Sci Inf Secur 14(9):938

Reddy GT, Meenakshi N (2014) Extended and embedded visual cryptography. Int J Comput Sci Mob Comput 3(2):235–247

Revathy S (2014) Secure crypto system for image encryption and data embedding using chaos and BB equation algorithm. Int J Comput Sci Mob Comput 3(3):297–306

Sanyasi Naidu P, Kharat R, Tekade R, Mendhe P, Magade V (2016) E-voting system using visual cryptography & secure multi-party computation. In: 2016 International Conference on IEEE Computing Communication Control and automation (ICCUBEA). IEEE, Pune, pp 1–4

Shaheen AM, Sheltami TR, Al-Kharoubi TM, Shakshuki E (2018) Digital image encryption techniques for wireless sensor networks using image transformation methods. DCT and DWT. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-018-0850-z

Shankar K, Eswaran P (2015a) ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J ApplEng Res 10(55):1841–1845

Shankar K, Eswaran P (2015b) Sharing a secret image with encapsulated shares in visual cryptography. Procedia Comput Sci 70:462–468

Shankar K, Eswaran P (2015c) A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique. Aust J Basic Appl Sci 9(36):150–163

Shankar K, Eswaran P (2016a) RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. J Circuits Syst Comput 25(11):1650138

Shankar K, Eswaran P (2016b) A new k out of n secret image sharing scheme in visual cryptography. In: 2016 10th International conference on intelligent systems and control (ISCO). IEEE, pp 1–6

Shankar K, Eswaran P (2016c) An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In: Artificial intelligence and evolutionary computations in engineering systems. Springer, New Delhi, pp 705–714

Shankar K, Eswaran P (2017) RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Commun 14(2):118–130

Shankar K, Lakshmanaprabu SK (2018) Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. Int J Eng Technol 7(1.9):22–27

Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A (2016) Multiple watermarking technique for securing online social network contents using back propagation neural network. Future Gener Comput Syst 86:926–939. https://doi.org/10.1016/j.future.2016.11.023

Singh L, Singh AK, Singh PK (2018) Secure data hiding techniques: a survey. Multimed Tools Appl,. https://doi.org/10.1007/s11042-018-6407-5

Sokouti M, Zakerolhosseini A, Sokouti B (2016) Medical image encryption: an application for improved padding based GGH encryption algorithm. Open Med Inform J 10:11–22

Srivastava R, Kumar B, Singh AK, Mohan A (2018) Computationally efficient joint imperceptible image watermarking and JPEG compression: a green computing approach. Multimed Tools Appl 77(13):16447–16459. https://doi.org/10.1007/s11042-017-5214-8

Talarposhti KM, andJamei MK (2016) A secure image encryption method based on dynamic harmony search (DHS) combined with the chaotic map. Opt Lasers Eng 81:21–34

Thakur S, Singh AK, Ghrera SP, Mohamed Elhoseny (2018a) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed Tools Appl:. https://doi.org/10.1007/s11042-018-6263-3

Thakur S, Singh AK, Ghrera SP, Mohan A (2018b) Chaotic based secure watermarking approach for medical images. Multimed Tools Appl:. https://doi.org/10.1007/s11042-018-6691-0

Toughi S, Fathi MH, Sekhavat YA (2017) An image encryption scheme based on elliptic curve pseudo-random and advanced encryption system. Signal Process 141:217–227

Vengadapurvaja AM, Nisha G, Aarthy R, Sasikaladevi N (2017) An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia Comput Sci 115:643–650

Younes MAB (2016) Literature survey on different techniques of image encryption. J Sci Eng Res 7(1):93–98

Zhang Q, Xu D (2018) Security authentication technology based on dynamic Bayesian network in Internet of Things. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-018-0949-2

Zhang J, Wang B, Xhafa F, Wang XA, Li C (2017) Energy-efficient secure outsourcing decryption of attribute based encryption for mobile device in cloud computation. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-017-0658-2

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