International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Secret Image Sharing Scheme Based on Pixel Segmentation Strategy Exploiting Modification Direction (PSSEMD) with High Quality Shadows

S. Lakshmi Narayanan, K. Sankaranarayanan, V. Vijayakumari

***Abstract**— Schemes of sharing a secret image are enhanced practically. The secret images are wrapped in cover imageon producing shadow images in this proposed scheme. In sequence,security is attained by means of methods of encryption and decryption while processing of sharing image. In the sharing step, cover image wrapped out the secret image by producing n images of shadow like cover image. This research dedicates a method of Improved Exploiting Modification Direction (IEMD) to conceal confidential data on preserving a high PSNR value. Pixel Segmentation Strategy EMD (PSSEMD) Method is used for wrapping confidential bit on all pixel cover image. the images as secret and cover are rebuilt by Shadow images. Lossless recovery of secret image is enriched by rebuilding the confidential image with lossless whereas by compressing the image before encryption and watermarking. Here Lossless image compression is done with the concern of sensitive information. Then chaotic encryption and decryption method is used for better security during image sharing process. Hence better embedding capacity and better quality in visual are attained in this proposed research results ensuring high security results in term of higher PSNR, lower MSE and higher correlation than the existing methods.*

***Keywords:** Threshold Secret Sharing, Confidentiality, Transformation, Compression, Secret Image, Exploiting Modification Direction; Binary Image*

I. INTRODUCTION

Handling confidential information in a public network like internet is not easy. It is not safe to store the secret information on a system which can be accessed by multiple users. Even if the secret information stored in a system which is protected with a password also, there may be a single point of failure [1].

It is not completely protected because multiple users will have the password. It may be misused or compromised by one or multiple users without the knowledge of other users. This compromises the confidentiality of the information. If the secret information needs to be transmitted over a network, it cannot be sent as it is over a network. There is couple of reasons for this restriction. One reason is the bandwidth required to send the information. Second reason is the issue about securing the confidential data transmission ended the network.

In 1979, accordingly of Blakley [2] and Shamir [3] sharing of confidential information is focused. Naor and Shamir [4] in 1995, on account of image applications, sharing of confidential data over image is termed as visual secret sharing that followed much in all applications. Recovery of the secret image with specific sharing of images in stego in confidential transmission of image by split up steps.

Communication channels are monitored to prevent the secret image sharing attack while transmission or storing in substitute of images. Thus security is ensured while transmission or storage in applications of commercial, financial etc., effectively [4].

Sharing field of the secret image is focused in maximizing the embedding capacity. Without imperceptibility changes in cover images wrapped up with huge secret data is referred as the embedding capacity.

Embedding of many secret information is possible by a given cover image with embedding capacity in huge scheme. Hence, embedding of large image in small cover image is good is referred as good embedding capacity scheme with less time and space consumption either in transmission or storage [5, 6].

In applications of [7], Embedding of much secret information in cover image and its capacity is lighter than threshold value. In Lin and Chan [8] application, the embedding capacity is further improved in 2010 by the sharing of confidential image wrapped in image cover and the embedding capacity size in scheme must be lesser. According to survey, Lin and Chan's application is good applicable with some pitfalls. Situations of overflow and underflow are seen in Lin and Chan's scheme [8].

Manuscript published on November 30, 2019.
* Correspondence Author

S. Lakshmi Narayanan*, Assistant Professor, Electronics and Communication Engineering, Sri Ramakrishna Engineering College, Coimbatore., Tamil Nadu, India.(Email: shrinarayanan20@gmail.com)

Dr.K. Sankaranarayanan, Dean, Department of Electronics and Communication Engineering, P.A. College of Engineering and Technology, Puliyampatti, Pollachi, Tamil Nadu, India. .(Email: kkdcbesankar@gmail.com)

Dr.V. Vijayakumari Professor, Department of Electronics and Communications Engineering,Er.Perumal Manimekalai College of Engineering, Koneripalli, Hosur, Tamil Nadu, India.(E-mail:ebinviji@rediffmail.com)

Pixel value of image may go increase of grayscale boundary that fails in result of lossless compression so that the cover image does not reveal the secret image.

Currently, [9] used an application by Chang et al. to overcome such an issue via several approaches. Situations of overflow and the underflow are focused more and capacities of the embedding schemes [7] are achieved less than Lin and

Chan's scheme. However the secret image in sharing mode enhance to improve the capacity of embedding schemes by minimizing situations of overflow and the underflow.

Thence, the developed proposal effort utilizes more secure method for privacy maintenance for controlled image sharing technique. In process of image sharing scenario, method of reversible data hiding is designed and developed for security purpose.

In sequence, segmentation of sensitive portion of images is watermarked. Thus enhancement of protecting sensitive information is performed to maximize the experimental result. Pixel Segmentation Strategy EMD Method is proposed in this proposal on exploiting modification direction for a scheme of sharing in secret image along good shadows based quality. This achieves shadow image covering with good quality by lossless image covering and sharing image.

II LITERATURE SURVEY

A scheme of (2, 2) visual secret sharing is designed by Wu and Chang [10] for reducing rotating angles iterations by adjusting circular shares. It achieves better result in sharing of two secret images. Since lossy reconstruction of image is appeared, low revealed secret images are obtained.

A scheme of (k,n) threshold secret image sharing is designed in [11] by encrypting a secret image into n image-shadows compromising k image-shadows with lower information on the image and reconstructing entire image by any k or more image-shadows.

Traditional secret sharing scheme faces Cheating problem majorly. Sharing of secret image must focus on this by constructing a scheme of secret image sharing holding a value of (k,n) threshold for detection of cheating.

The cheating behavior from up to $k-1$ cheaters are detected by proposed scheme and the size of image-shadow are similar as the image-shadow in the original secret image sharing scheme.

The PVO method is designed by Li et al. (2013) [12]. The pixel vector gets reordered pixels and identifies the smallest pixel by second smallest pixel and identifies the largest pixel by second largest pixel accordingly in this method. Prediction errors 1 and −1 are used to data incorporation remaining constant prediction error 0. image redundancy are reduced in Peng et al. (2014) by enhancing PVO method for incorporating larger blocks and attains a higher PSNR [13].

The PVO method is modified by Qu and Kim (2015) for prediction of each pixel by its sorted context pixels for obtaining image regions to achieve a better embedding capacity [14]. A strategy of dynamic blocking by Wang et al. (2015) is done to division of the cover image into various-sized blocks. a high embedding capacity is achieved by dividing the flat image areas into smaller blocks by dividing rough areas into larger blocks to minimize the decrease of PSNR value [15].

EMD method by Zhang and Wang (2006) [16] produce quality image with greater than 52 dB for the stego-image with a peak signal-to-noise ratio (PSNR) with one pixel either increasing or decreasing in each pixel group. Further, the EMD method is enhanced by Kieu and Chang (2011) by exploring amendment directions of eight to incorporate many undisclosed bits into a cover pair at a time [17].

III PROPOSED METHODOLOGY

Hence proposal of developed system uses reversible data hiding for high security over sharing of image efficiently. This is the approach of one hiding techniques for lossless covering of image along with extraction of secret message precisely.

The proposal of research contains three main phases such as segmentation of sensitive parts of image, threshold scheme for better encryption and decryption process and PSSEMD method for secret image sharing information, Chaotic method for higher security and access control.

A. Segmentation of Sensitive Parts of Image

An input click of image includes needed image along with noisy data and unwanted background contents too.

Memory challenges are to be sorted out in storage for clearing these noisy and unwanted content and bandwidth issues on image sharing. In order to prevail over these challenges image segmentation are done on sensitive part of entire image and summed up.

It segregates image of foreground from the background stills. The designed research performs segmentation of classification in learning optimised to switch methods of segmentation. In segmentation of an image, classification which is pixel based learning and region based learning is considered from current approaches.

B. Markov Random Fields (MRFs)

Markov Random Fields (MRFs) [18] taken as delegate case and classification of learning-based region. As determined from MRFs, either at the level of the pixel or at patch plane focusing scale of predefined spatial (size), then images are partitioned into various sites.

each site determines: (i) a hidden node or label node, evaluates the specific a hoped node: a region of interest or background is referred as region segmentation, (ii) node on observation or feature, determines feature set of the site, which is predicted in a clear-cut side from images. So the segmentation result leads to global issue of optimization, that is, foresee the field of label which is desired from the scrutiny. Deterministic energy minimization approach is carried out for conventional deformable models in sequence. Thus predominate result are not produced and so the probabilistic solution is determined in the developed research of learning-based classification methods for obtaining the maximization of probability.

C. Apply Threshold Scheme for Better Encryption and Decryption Process

Polynomial interpolation is implemented in the approach developed by Shamir's threshold secret sharing [2].

Key is reconstructed by Lagrange's interpolation. sharing method is implemented for distributing the confidential data among multiple user using the polynomial of the order m-1 for (m,n) secret sharing for producing shares. Value of threshold is denoted by m and number of authorized users influence n total number of shares. The polynomial is

$$f(x) = S + Cx + Cx^2 + Cx^{m-1} \qquad (1)$$

Where secret is S, to be shared among n users. Selection of coefficients are C1, C2, C3 done randomly. Using this

polynomial and selecting unique values for x, the dealer divides the secret in to number of shares.

$$f(x_1) = y_1, (x_2) = y_2 ,..., f(x_n) = y_n \qquad (2)$$

Where $y_1, y_2, \dots\dots y_n$ are generated share. Authorized users get the share value x but not key construction by dealer. x_i and y_i are value pair by all user.

On reconstructing the information by the user, sharing from other users are influenced. In sequence of obtaining m shares number reconstruction of information are performed by user. Thus ensure no leakage of information while sharing significantly and confirms no possibility of sharing information if m number of shares are lower. Key construction is possible if there is minimal m shre number. It ensure security by attackers not share information. any authorized user wont miss any opportunity and protect from attacker.

Lagrange's interpolation performs the reconstruction of the secret to resolve the S coefficients specifically. The interpolation formula is:

$$f(x) = \frac{(x-x_1)(x-x_2)y_0}{(x_0-x_1)(x_0-x_2)} + \frac{(x-x_0)(x-x_2)y_1}{(x_1-x_0)(x_1-x_2)} + \frac{(x-x_0)(x-x_1)y_2}{(x_2-x_0)(x_2-x_1)} + \cdots \dots \qquad (3)$$

Solving equation (3) produces result in S.

This is a perfect secret sharing, because the secret S is reconstructed only with m or greater than shares m. It is not possible to reconstruct ke on presence of lower value m.

D.Improved Exploiting Modification Direction (IEMD) Method Using Pixel Segmentation Strategy for Secret Image Sharing

a traditional scheme of sharing secret (*t*, *n*) posses true dealer and participants *n*. Like a traditional scheme of sharing secret, it also possess and identifies indices ID_i, for *i*=1, 2,…,*n* . in a scheme of sharing secret, *n* images shadow are produced by the dealer wrapped from the secret image enclosed in the cover image. It despatches *n* participants over a secure channel. On occasion of sharing the image by more than t or t members, then cover and secret image are shared. Hence secret image sharing mechanisms is performed by EMD method and the shadow images are produced by 2-dimensional hyper-cubes [19]. The proposed research attains low distortion and lossless reconstruction.

gray scale cover image is represented by *O inclusive of* pixels $M \times N$, let $O = \{O_i | i = 1,2, \dots, (M \times N)\}$, and let *S* be a shared secret gray scale image (among *n* participants) that has $H \times W$ pixels.

Lagrange interpolation polynomial influences the dealer for (*t*, *n*) threshold secret sharing scheme for producing *n* meaningful image shadows, denoted S_i, for *i*=1, 2,…, *n*.

The proposed research hold three steps as (1) the preliminary phase, (2) the derivation of shadow phase, and (3) retrieving phase of the secret image. These steps are detailed below.

Preliminary Phase

Step 1. a size of 255× 255 in hyper-cube of 2-dimensional are produced.

coordinate figures acts as x-axis and grayscale image and its pixel value acts as y-axis. Thus in hyper-cube of a 2-dimensional, 5-ary notational system digitare mapped with a pixel pair.

Step 2. 5-ary notational systems are attained from transformed secret image pixel like EMD method. divide the shared image S in bit stream into 5 $H \times W \times \lceil \log_5 255 \rceil$ non-overlapping segments. Then, S can be denoted as

$$S = \{s_j | j = 1,2, \dots, (H \times W \times \lceil \log_5 255 \rceil)\} \quad (4)$$

Shadow Derivation Phase

Multi-secret sharing scheme reconstructs Lagrange interpolation polynomial to *t* shadow images by YCH (*t*, *n*).

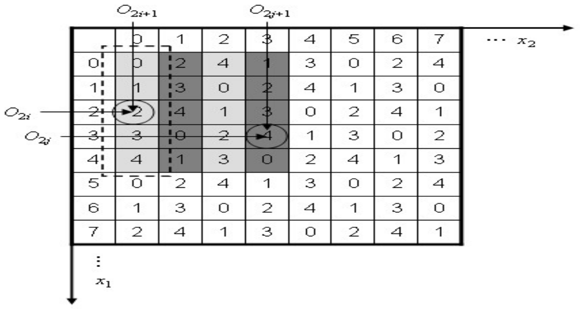
Considering t as threshold value and O is (O_{2i}, O_{2i+1}) as the selected camouflage pixel pair, the steps as below generate the shadows.

Step 1: five successive squares which is small in size of blocks obtained from a division of 2-dimensional hyper-cube. These five successive squares embed the shadow images from secret image using of blocks.

Although, the 256× 256 squares is wrapped in 2-dimensional hyper-cube, blocks does not hold a special point for messages not hidden by pair of pixel accordingly.

The point is evaluated by several experiments resulting in less the embedding capacity and quality in visualisation of image shadowing. In cover image, special point as pixel pair(175, 255) are selected that helpless for cover image selection. In the horizontal direction, partition is done along bottom line. Certainly not this a way of splitting up Of 2-dimensional hyper-cube.

Step 2. Mapping out (O_{2i}, O_{2i+1}) along with 2-dimensional hyper-cube produces a 5-ary notational digit. d_i Represents the 5-ary notational digit. Here the proposed research represent C as the mapping function from pixel pair (O_{2i}, O_{2i+1}) to the notational digit of 5-ary d_i, $C(O_{2i}, O_{2i+1}) = d_i$. We define the function C^{-1} as $C^{-1}(d_i) = (O_{2i}, O_{2i+1})$. According to the characteristics of the 2-dimensional hyper-cubes, five different values from 0 to 4 present in the specific block including the point d_i. As shown in Figure 1, $C(O_{2i}, O_{2i+1}) = d_i = 2$ and in a frame , dashed box helps to design the block.



	0	1	2	3	4	5	6	7
0	0	2	4	1	3	0	2	4
1	1	3	0	2	4	1	3	0
2	2	4	1	3	0	2	4	1
3	3	0	2	4	1	3	0	2
4	4	1	3	0	2	4	1	3
5	0	2	4	1	3	0	2	4
6	1	3	0	2	4	1	3	0
7	2	4	1	3	0	2	4	1

Figure 1: Instance of shadows derivation

Step 3. *t* 5-ary notational digits are used by lossless of $d_i, s_1, s_2, \dots s_{t-1}$, secret image of 5-ary notation represents $s_1, s_2, \dots s_{t-1}$, degree polynomial (*t*-1)th construction.

$f(x) = d_i + s_1 x + s_2 x^2 \dots + s_{t-1} x^{t-1} \text{ mod } 5.$ (5)

Step 4. identifying index ID_j *are present in all* participant. the ID_junique index are fed in *f* (*x*) , for *j*=1,2,…,*n* for dealer calculation *n* pairs of $(ID_j, f(ID_j))$ determined by Step 5. From the block located by d_i , we obtain the embedded pair (O_{2i}^j, O_{2i+1}^j) by computing $C^{-1}(f(ID_j))$, For $j = 1,2,\dots,n.\ (O_{2i}^j, O_{2i+1}^j)$.

Then the shadow image is according pixel pair

Step 6.Iteratively, secret image are embedded into the *n* shadow images S_i.

Pixel Segmentation Strategy EMD Method

pixel segmentation strategy supports to improving EMD method by Lee et al. approach on wrapping large payloads [10]. In this research, $(2n+1) - ary$ notational system of pixel segmentation strategy is hold by couple of cover image. a vector of coordinates (VCA) and a coordinate vector modification area (VMA) are primary embed method of cover data. g_i and g_j are two pixel group holding bits inside pixel efficiently where g_i^{msb} , g_j^{msb} , g_i^{lsb} and g_j^{lsb} are represented as least significant bits. $g_i^{msb} + g_j^{msb}$ bits are referred as VCA and VMA are the $16 - \left(g_i^{msb} + g_j^{msb}\right)$ bits. Eq. (2) calculates the sub clusters with positive integer n of VCA to retrieve f function.

No need of change is required if f is equivalent to d secret digit d. For the difference value $s = d - f$, when s is greater than n, the value of sub-group $g_{(2n+1)-s}$ has to be logically decreased by one, otherwise the value of g_s has to be increased by one. The embedding rate $\mathrm{R} = \log_2(2\mathrm{n}+1)/2$ was greater than that of $\mathrm{R} = \log_2(2\mathrm{n}+1)/\mathrm{n}$ which the EMD embedding method proposed when n got larger without loss of quality and security. Hence this approach provides a high quality for the resulted image, it is possible to improve the embedding capacity.

one cover pixel carries the central technique of data hiding method that holds (2n+1)-ary notational secret digit in a system. By using one pixel for cover data, the method achieves a capacity double that of the EMD method.

Embedding Procedure

For a pixel value, g_i on each cover data, the function value f is calculated by Eq. (5), where $|x| \leq n$. If the value of a pixel falls between $0 \leq g_i \leq 1$ and $254 \leq g_i \leq 255$ for each, then x is selected satisfying the condition $0 \leq x < 2n+1$ and $-(2n+1) < x \leq 0$ respectively.

A new pixel value g_i' is obtained by above eq, where the value of x is selected to satisfy the f=d condition.

$g_i' = g_i + x$ (6)

In the extraction method, a secret digit d is calculated by Eq. (7).

$d = g_i' mod(2n+1)$ (7)

Secret Image Retrieving Phase

Original image O is rebuilt with S shared secret image in scheme of Shamir's threshold along t shadow images $S_j's$. Shadow images S_j , for j=1,2,…, t with lossless generality and any of t participants is ready to rebuilt the secret image.

Technique of cheater identification verifies the shadow images that also detect duplicate participant is not identified in this work. Cover image inclusive of pixel pair (O_{2i}, O_{2i+1}) is reconstructed and through t shadow images it wrap out secret data. Rebuilding of the cover image and the secret image data are done iteratively.

Step 1. shadow images 't' produce (O_{2i}^j, O_{2i+1}^j), for *j*=1, 2,…,*t*, are the pixel pairs. unique index D_j gives similar 2-dimensional hyper-cube to produce $f(ID_j)$ by mapping the column O_{2i}^j and the row O_{2i+1}^j .

$f(ID_j) = C(O_{2i}^j, O_{2i+1}^j)$, where j=1,2,...,t.

Step 2. Lagrange interpolation polynomial reconstructs with lossless generality and *t* pairs $(ID_j, f(ID_j))$, for *j*=1,2,…, *t*, the (*t*-1)th degree polynomial $f(x) = d_i + s_1 x + s_2 x^2 \dots + s_{t-1} x^{t-1}\ mod 5$

Step 3. For 5-ary notational digit d_i of the cover image and the, for i=1,2,...,t-1,shared secret image data s_i *is attained* from the pixel pair. $(O_{2i}, O_{2i+1}) = C^{-1}(d_i)$ is evaluated to find pixel pair (O_{2i}, O_{2i+1}) of the cover image

Step 4. Cover and secret images are retrieved from above steps iteratively.

E Chaotic Method for Higher Security and Access Control

In this work, the chaotic method is applied for ensuring the security in higher and it is used for better access control to the authorized users. image encryption technique are focused here in this recent research by Chaos. Yet, precision of finite computational gives reconstruction of chaotic sequences. A strong image encryption algorithm is performed for incorporation of permutation and substitution methods. two sub processes are carried out in the encryption of each bitplane by constructing a chaotic ergodic matrix for permutation of bit positions and bit values substitution are done by producing two binary chaotic pseudorandom sequences [20]. Initially, sequence generator adopts a function in single direction for damping reverse prediction and in sequence, the recursive relations are eliminated by forwarding a cross-ampling method on segregating binary chaotic pseudorandom sequences. Hence, experimental results predict high mechanism of security in mixed encryption method.

couple (J, f) determines a one-dimensional discrete-time nonlinear dynamic system with real interval by J and nonlinear iterative scalar transform by f:

$x_{i+1} = f(x_i)$ (8)

Where $\{x_i\}$ is the chaotic sequence generated by $f.x_i(i \geq 0)$ determines the states of the dynamic system and x_0 denotes the initial condition.

Logistic map is widely popular and used as

$f(x) = \mu x(1-x), \quad x \in (0,1)$ (9)

The Logistic sequence of probability density function is represented as

$$\rho(x) = \begin{cases} \frac{1}{\pi\sqrt{1-x^2}} & 0 < x < 1 \\ 0 & otherwise \end{cases} \quad (10)$$

The encryption algorithm can be described as follows:

Step1. a chaotic systems with its origin values are selected.

Step2. Eight bitplanes are attained by decomposition of original image

Step3. eight ergodic matrices are constructed with the optimized chaotic sequences by generation of chosen initial values accordingly. bitplanes are permuted by ergodic matrices.

Step4. bitplanes are combined Renewably to attain permuted image from encrypted image.

Step5. Chen's chaotic system encrypts the permuted image pixel values

The process of decryption is obvious. on the other hand encryption process gets executed to produce the decrypted image.

These steps are iterated and implemented in the MATLAB environment that explored detail in forthcoming sections. Security and access control in efficient are obtained through this procedure.

IV EXPERIMENTAL RESULTS

MATLAB specifically, programming language is supported for achieving experimental results in better numerical and computing application. Linear algebra is achieved by a computer environment with similar notation of language. The following parameters Peak signal to noise ratio, Mean squared error and Maximum embedded capacity are considered in the proposed methodology against existing system by ensuring the security level.

The proposed research methodology Pixel Segmentation Strategy EMD (PSSEMD) Method against prevailing approaches for secret image data security to base fact of encryption and watermark or CIDSEW [21], chaos encryption [22], Flash DRM [23] are done. The statistical evaluation is specified in graphical formats.

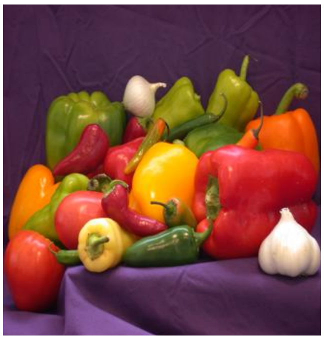


Figure 2: Input image

The proposed methodology takes Figure 2 as input image for the transmission of confidential and hidden message.

Proposed scheme is proven to best here of section via experimental results. Shadow images with the visual quality in various modulation of fifteen grayscale images are considered for experimentation as the cover images. pixels of 256× 256 secret sharing image are detailed in figure 3. The value of n and t is set to value 4.

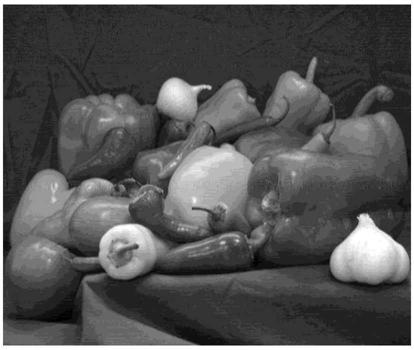


Figure 3: secret image

Figure 2 segmented image of input are sealed in figure 3 as confidential images wrapping of secret message

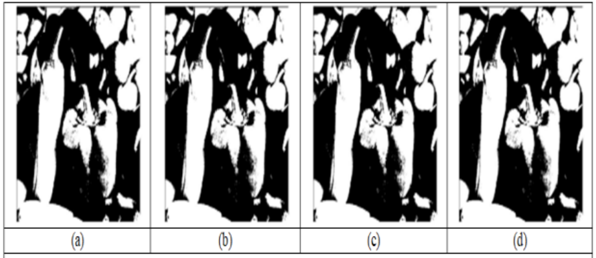
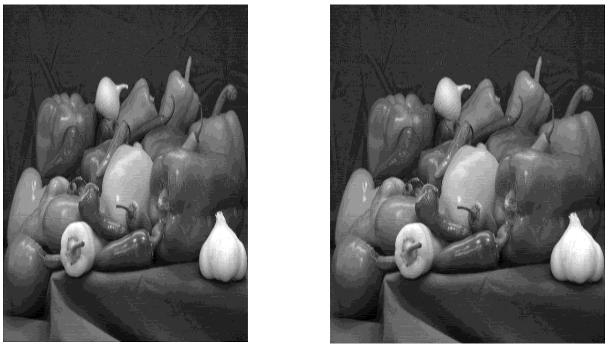


Figure 4: Shadow images, The results of pepper image, n=4 and t=4

Pixel value of 512×512 in grayscale image as the cover image is used to explore shadow images in visual quality wrapping of pixel value of *pepper* 256× 256 enclosing confidential image. *pepper* with four shadow images are pictures in Fig. 6(a-d) and *pepper image in lossless distortion of retrieved confidential image are pictures in* Fig. 5(a) and lossless image in in Fig. 5(b).



a)cover image **b)reconstructed loss lessly image**

Figure 5: Reconstructed Image

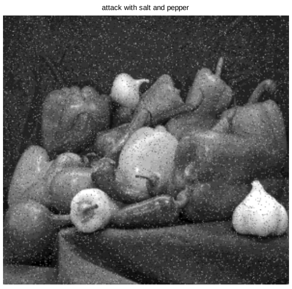


Figure 6: Salt and pepper attack image

Accurate image is retrieved after decryption of noise image enclosed with noise of salt and pepper are pictures in Figure 6.

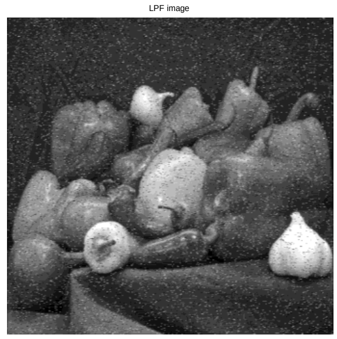


Figure 7: Noise removed image

The image before decrypt i.e., noise removal image are pictures as noise removed image in Figure 7.

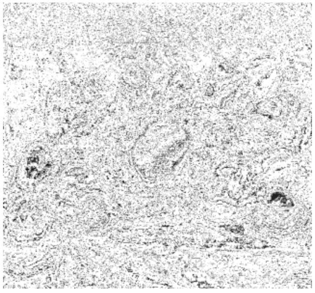


Figure 8: Decryption image

The received secret message that to be decrypt are pictures in Figure 8.

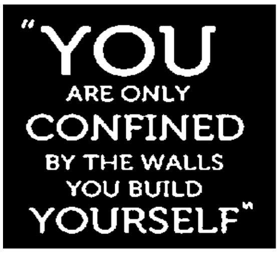

"YOU
ARE ONLY
CONFINED
BY THE WALLS
YOU BUILD
YOURSELF"

Figure 9: Decryption of image

The image of input enclosed in hidden secret message as image decrypted are pictures in Figure 9.

Peak Signal-To-Noise Ratio (PSNR)

Image or video recreated and its quality are measured by PSNR. The ratio of input image or video as high end possible power to the power of output image or video is referred as PSNR.

$$\mathrm{PSNR} = 10\log_{10}(\mathrm{MAX}_i^2/\mathrm{MSE}) \quad (11)$$

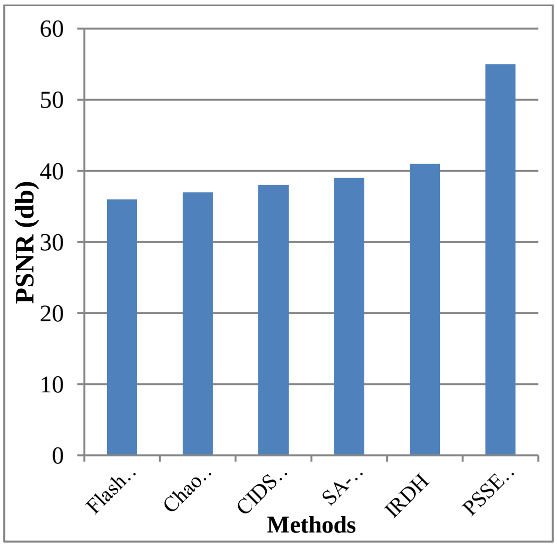


Figure 10: PSNR

Figure 10 explains the experimental results of PSNR for proposed against prevailing methods. Methods and values of PRNR are plotted as x and y-axis accordingly. The proposed method achieves higher PSNR than prevailing methods as Flash DRM, Chaos encryption, CIDSEW, SA-UAC and IRDH algorithms. The image quality is enhanced by the proposed PSSEMD approach securely.

Mean Square Error

The variation between an estimator and estimated quantity true value are calculated by estimator of Mean square error (MSE).

$$\mathrm{MSE} = \frac{1}{m\times n}\sum_{k=0}^{m}\sum_{l=0}^{n}[f(k,l) - f'(k,l)]^2 \quad (12)$$

while

host video is represented by f (k,l) and embedded/ extracting image by f '(k,l).

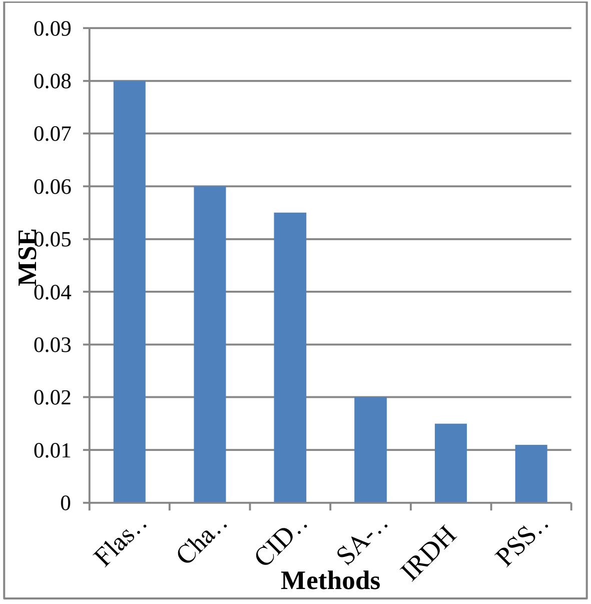


Figure 11: MSE

Figure 11explains the experimental results of MSE for proposed against prevailing methods. Methods and values of MSE are plotted as x and y-axis accordingly. The proposed method achieves lower MSE than prevailing methods as Flash DRM, Chaos encryption, CIDSEW, SA-UAC and IRDH algorithms. The image quality is enhanced by the proposed PSSEMD approach securely.

The Maximum Embedded Capacity with Different t

The embedding capacity is the ratio of maximising threshold t to the PSNR value of the shadow images reaches a good level.

Polynomial degree is high accordingly with maximum value of threshold is tabularised in Table 1.

Table 1: Embedded capacity with Different

t	Capacity (secret pixels	PSNR (Db)
4	313×313	45.01
6	404×404	45.18
8	478×478	44.95
1 0	543×543	45.11

Correlation

Two variables to each other with relationship in linear are extended and referred as Correlation in statistical relationships entailing dependence.

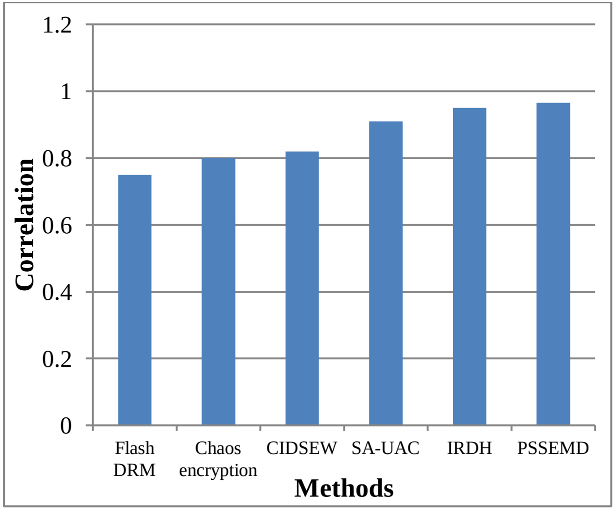


Figure 12: correlation

Figure 12 explains the experimental results of correlation for proposed against prevailing methods. Methods and values of correlation are plotted as x and y-axis accordingly. The proposed method achieves higher correlation than prevailing methods as Flash DRM, Chaos encryption, CIDSEW, SA-UAC and IRDH algorithms. The image quality is enhanced by the proposed PSSEMD approach securely

V CONCLUSION

Multiple users and multiple servers utilises the high confidentiality transmission of image using proposed method enclosing the secret image. The confidential information is protected by a method of a secret sharing are widely used by multiple users. The secret are reconstructed by sharing quantity of threshold value enriches the threshold secret sharing.

Based on exploiting modification direction, new (t, n)-threshold secret image sharing scheme along with steganographic properties are incorporated with Shamir's secret sharing method. the pixel pairs ($O2i$, $O2i$+1) and the 2-dimensional hyper-cubes are constructed by an injective map. The shadow images are attained by sealing secret data on cover image using the injective map. The lossless output image are extracted with maximum quality by shadow imaging that sealing secret data in cover image in the proposed scheme and additionally applied to binary images. Security is ensured by encryption and decryption of Chaotic. The experimental result proves that the proposed PSSEMD method provides higher PSNR, lower MSE, higher security level and higher correlation metrics rather than the existing systems..

REFERENCES

1. R. Calderbank, I. Daubechies, W. Sweldens, and B.- L. Yeo. Lossless image compression using integer to integer wavelet transforms. In Proc. ICIP-97, IEEE International Conference on Image, volume 1, pages 596–599, Santa Barbara, California, Oct. 1997.
2. Blakley G. R. Safe guarding cryptographic keys. Proceedings of the 1979 National Computer Conference; June 1979; pp. 313–317. [Google Scholar]
3. Shamir A. How to share a secret. Communications of the ACM. 1979; 22(11):612–613. doi: 10.1145/359168.359176. [Cross Ref] [Google Scholar]
4. Naor M., Shamir A. Advances in Cryptology—EUROCRYPT '94. Berlin, Germany: Springer; 1995. Visual cryptography; pp. 1–12. [Cross Ref] [Google Scholar]
5. Lin C.-C., Tsai W.-H. Secret image sharing with steganography and authentication. Journal of Systems and Software. 2004;73(3):405–414. doi: 10.1016/s0164-1212(03)00239-5. [Cross Ref] [Google Scholar]
6. Wu Y.-S., Thien C.-C., Lin J.-C. Sharing and hiding secret images with size constraint. Pattern Recognition. 2004;37(7):1377–1385. doi: 10.1016/j.patcog.2004.01.002. [Cross Ref] [Google Scholar]
7. Ulutas M., Ulutas G., Nabiyev V. V. Invertible secret image sharing for gray level and dithered cover images. Journal of Systems and Software. 2013; 86(2):485–500. doi: 10.1016/j.jss.2012.09.027.
8. Lin P.-Y., Chan C.-S. Invertible secret image sharing with steganography. Pattern Recognition Letters. 2010;31(13):1887–1893.
9. Chang C.-C., Lin P.-Y., Wang Z. H., Li M. C. A sudoku-based secret image sharing scheme with reversibility.
10. H.C. Wu, C.C. Chang, Sharing visual multi-secret using circle shares, Comput. Stand. Interfaces 28 (2005) 123–135.
11. Yan-Xiao Liu, Qin-Dong Sun and Ching-Nung Yang, "(k,n) secret image sharing scheme capable of cheating detection", EURASIP Journal on Wireless Communications and Networking20182018:72
12. Li, X.; Li, J.; Li, B.; Yang, B. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. Signal Process. 2013, 93, 198–205. [Cross Ref]
13. Peng, F.; Li, X.; Yang, B. Improved PVO-based reversible data hiding. Digit. Signal Process. 2014, 25, 255–265.
14. Qu, X.; Kim, H.J. Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding. Signal Process. 2015, 111, 249–260. [Cross Ref]
15. 14. Wang, X.; Ding, J.; Pei, Q. A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition. Inf. Sci. 2015, 310, 16–35. [Cross Ref]
16. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett. 2006, 10, 781–783. [Google Scholar] [Cross Ref]
17. Kieu, T.D.; Chang, C.C. A steganographic scheme by fully exploiting modification directions. Expert Syst. Appl. 2011, 38, 10648–10657. [Google Scholar] [Cross Ref]
18. R. Huang, V. Pavlovic, D.N. Metaxas, A tightly coupled region-shape framework for 3D medical image segmentation, IEEE International Symposium on Biomedical Imaging: Nano to Macro, Arlington, VA, USA, 2006, pp. 426-429,
19. Guo, Cheng, Zhi-hui Wang, Chin-Chen Chang, and Chuan Qin. "A Secret Image Sharing Scheme with High Quality Shadows Based on Exploiting Modification Direction." Journal of multimedia 6, no. 4 (2011).

20. Enayatifar, Rasul, Abdul Hanan Abdullah, and Ismail Fauzi Isnin. "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence." Optics and Lasers in Engineering 56 (2014): 83-93.
21. Qian, Zhenxing, et al. "Block cipher based separable reversible data hiding in encrypted images." Multimedia Tools and Applications 75.21 (2016): 13749-13763.
22. Hong, Wien, Tung-Shou Chen, and Han-Yan Wu. "An improved reversible data hiding in encrypted images using side match." IEEE Signal Processing Letters 19.4 (2012): 199-202.
23. Desai, Chaitanya, Deva Ramanan, and Charless C. Fowlkes. "Discriminative models for multi-class object layout." International journal of computer vision 95.1 (2011): 1-12..