HYBRIDIZATION OF VISUAL CRYPTOGRAPHY AND IMAGE REALIZATION STEGANOGRAPHY

Sandeep Gurung^{1*}, Pooja Rai², Harsh Sikhwal³, Muksam Limboo⁴
and M K Ghose⁵

^{1,2,3,4}*Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology, Sikkim Manipal University, India*

⁵*Department of Computer Applications, Sikkim University, Sikkim, India*

¹sandeep.gu@smit.smu.edu.in, ²poojasampangrai@gmail.com,

³harsh.astro1996@gmail.com, ⁴muksamchong105@gmail.com,

⁵mkghose@cus.ac.in

Abstract— In the world of information technology our dependence on it have increased manifolds. The dynamic nature of the web, its complexity and communication over unsecure communication channel (internet) augments additional problems giving rise to many security concerns namely secrecy and authentication. The paper focusses on the design of a hybrid architecture combining the attributes of visual cryptography and steganography, which can be used for many applications including polling, copyright protection, biometrics, etc. The multi-tier security model offers a hierarchical tree architecture for distributing information between authenticated participants. Random grid based visual cryptography scheme is extended for multiple secret hiding, the scheme can easily be decoded by using the Human Visual System. The noisy patterns/shares generated from visual cryptography are concealed in digital carriers for storing or for distributing the information to the rightful users. The proposed system maps and embeds the shares generated through image realization steganography to one of the CMY planes of the cover image. The statistical distribution of the pixel information of the image is used as a basis for the measurement of region identification for message embedding. A variable data rate embedding is used for mapping the information in the carrier image to reduce the distortion induced on the carrier image. The multi-level security model offers increased secure and is robust towards security attacks.

Keywords— Information Security, Authentication, Secrecy, Visual Cryptography Random Grids, Multiple Information Hiding, Image Realization, Hybridization

1. INTRODUCTION

With the explosive growth of the internet, large volumes of private sensitive data are exchanged through the unsecured communication channel every second which is highly susceptible to various categories of active and passive attacks. The growing need of the users and the additional burden of increasing new applications often demand change in the existing system and policies. Information security aims at preserving the primary goals of secrecy, authentication, and integrity through the design and uses of various algorithm and policies, to ensure that the security requirements are met at both ends [18]. Cryptography converts the actual data into non-intelligible form which facilitates in

Received: June 25, 2019

Reviewed: October 15, 2019

Accepted: February 4, 2020

shielding the information from unsolicited users. Authentication schemes in cryptography is achieved by the use of authenticators implemented through the uses of message digests and hash codes. The strength of these approach depends on the choice of the one way function used. Authentication is therefore highly structure (deceased flexibility) and use of mathematical functions (eg: Digital Signature Standard) often involve exchange of preliminary variables making it challenging to implement it on the web. Public cryptosystems also require the sharing of public certificates and the increasing size of prime number for better security further increases computational complexity. In similar trend, steganography hides the existence of secret data by concealing them into digital carriers which acts as an envelope for storage and distribution. The cover and the stego are visually identical and in any other form indistinguishable and do not indicate about the presence of any secret information. The requirements for these kinds of methodologies nowadays are becoming very crucial due to the increasing number of adverse methods posing serious challenges to the protection and distribution of sensitive information.

The $k : n$ visual cryptography secret sharing scheme [22] involves the distribution of secret information between 'n' shares/participants, wherein the overlapping of a minimum of 'k' shares are essential to decipher the information. These onetime pads (shares) are a perfect example of security as the shadows (shares) alone have insufficient information to decode the message. The scheme facilitates the construction of a sharing scheme where the dependence of a secret information is not confined to a single source/entity. The encoded information is reconstructed and interpreted by the Human Visual System by overlapping the shares/transparencies as shown in Figure 1.

Fig. 1 Code book generation for a (2, 2) Visual Cryptography Scheme
(pixel expansion = 4)

Traditional visual cryptography involves loss in contrast for the reconstructed image due to the involvement of pixel expansion and also affects the aspect ratio of the resultant image [22]. Generalization is difficult and the use of a code book as a reference for distributing pixel information in the shares further deteriorates the performance of the system. The carrying capacity of the scheme is limited and possible solutions to its limitations are addressed in section 2.2 in the paper. Random grids (RG) [7], a non-pixel expansion scheme overcomes the problem faced by traditional visual secret sharing scheme by distributing information uniformly in shares without using a code book. In a 2:2 random grid visual cryptographic secret sharing (RGVCSS) scheme, the black and white pixels are randomly and uniformly distributed across in the first share. The second share generation involves the participation of the first share and the secret information. Thus a visual cryptography scheme benefits with the involvement of only a single level of computation as the decoding can be done by using the Human Visual System. The

approach implements a perfect mechanism of a secret sharing scheme, e.g.: key distribution.

Steganography, an alternative, flawlessly hides the data into digital media known as 'cover'. It utilizes image, audio or video as carriers to achieve its goals. It exploits the properties of the carriers to conceal data and unlike cryptography the occurrence of the secret information cannot be perceived. Various spatial, frequency and statistical based steganography techniques have been suggested in [2] with the third variant having the best embedding efficiency. Image realization techniques exploit the statistical distributing of the carrier pixels for embedding information by mapping the secret data to the cover with decreased blockiness, hence more bits can be embedded with little change in the original pixel distribution. Different color models such as RGB, CMY, HSV etc. have been utilized as a platform to implement variants of covert writing techniques to map the secret information depending on the domain of use. Discrete Wavelet transform, a frequency based technique utilizes smooth and rough regions based on their standard deviation to implement the cover-to-secret mapping. The image blocks are randomly chosen for better diffusion and scattering of the message leading to little or no human detection.

Various hybrid models are suggested in [6, 25]; these techniques try to combine the best attributes of both the mechanisms to generate security systems which are more secure and robust towards attacks and the hybrid architecture complements each other. A hybrid model in [25] utilizes a Boolean function for efficient computation. In [6] embed the information encrypted using visual cryptography in the quantized DCT coefficients of an image to generate stronger stegos. Thus a need of a general hybrid model with high carrying capacity with acceptable contrast has been a burning question nowadays. Multi-tier security models provided an efficient solution by providing a platform that is robust and more resilient towards all forms of attack. Section 2 summarizes the related work in the field, Section 3 underlines the proposed methodology, the design in given in Section 4, Section 5 gives a brief discussion on the experimental results and the paper conclusion is given in Section 6.

2. RELATED WORK

2.1. VISUAL CRYPTOGRAPHY AND RANDOM GRIDS.

The 'k' by 'n' threshold visual cryptography scheme which involves pixel expansion initially proposed by Naor and Shamir [22] was built on the foundations of Lagrange's Interpolation [1], where the constant in the polynomial was represented as the secret message. For a 2: 2 scheme, the system generated 2 binary shares using a code book as mentioned in section 1. The information is reconstructed after overlapping one of the shares with the other in the correct orientation as given in Figure 2. The resultant image is bigger in comparison to the original image due to the involvement of pixel expansion.

Fig. 2 Traditional (2, 2) Visual Cryptography scheme. a) Secret Image, b) Shadow 1, c) Shadow 2, d) Restored Information

Random Grid (RG) as proposed by Kafri and Keren [7] belongs to a category of probabilistic visual cryptography. The non-pixel expansion based scheme distributes the

secret information over two random grids RG_1 and RG_2 . The first grid RG_1 contains a uniform random distribution of black and white pixels i.e. the probability of a pixel being white/black is equal to $1/2$. The pixels in the second grid RG_2 are decided by taking the secret and the grid RG_1 as a reference. Stacking of the two grids RG_1 and RG_2 finally reveals the secret information hidden. Three variations of the random grid formulation was suggested, algorithm 1 gave the best performance with a theoretical contrast of $1/2$ as shown in Figure 3.

Fig. 3 Implementation of Random Grid using Algorithm 1

The generalization of 'n' by 'n' scheme as suggested by Chen et al [13], involved the repetition of the basic algorithm for a creation of a tree of depth 'n' wherein one of the output shares of one level was taken as an input to another. To improve on the contrast of the restored image [15] which decreases with increase in the deepness of propagation of the tree, each pixel information of the grids of various levels were stored temporarily before being mapped randomly to the resultant grids. The contrast for an 'n' by 'n' scheme was found to be equal to $1/2n-1$. Tzung-Her Chen [16], in another paper suggested a way to control the dispersal of random black pixels in the shares. For occurrence of a white pixel in the secret image, a random function was used to assign the pixels values in the resultant shares. The likelihood of a pixel being black or white was evaluated as $1/n$ and $n-1/n$ respectively. For a k: n scheme, it generated an optimal contrast of $\alpha = (t-1)/(2*n-t)$, where 't' specifies the cardinality of the grids piled up together with $t \geq k$.

2.2. MULTIPLE INFORMATION HIDING USING RANDOM GRIDS

Multiple information hiding gave new directions in the field of Visual Cryptography for increasing the number of information encoded in the shadows/shares as the traditional approach had a limitation of encoding only a single secret. Wu and Chen [19] initiated the concept of multiple secret sharing in rectangular shares wherein one of the shares was rotated anti-clockwise at various angles of 90° , 180° and 270° to recover multiple secret information. The predictable angle of orientation was a major drawback of the approach.

Another popular approach for multiple secret hiding utilized the concept of recursive information hiding [8] where smaller secret were concealed in larger secrets. The shares of the smaller secret was concatenated to create shares of higher dimensions. Each share of 2^m bits can carry $2^{m+1} - 1$ bits of information, making the algorithm very efficient for share generation. Conversely, the increase in the share size added more burden to the communication channel for distribution.

Feng et al [5] methodology of concealing multiple secrets used a graphical construct of stacking rules to distribute the pattern of pixels in the shares. It involved the magnification of a single pixel to a 2 by 2 sub pixel, thus involving pixel expansion

which contributed to the loss in contrast. In Lina et al [14], the hamming weight of the shares based on pixel patterns was used to determine the distribution of pixels. To improve the contrast, the scheme involved a camouflaging process which ensured the uniform distribution of the black pixel in each of the shares. The number of secret information was limited to two.

Joy Jo Ying et al [21] used horizontal columnar shifts in the shares to hide multiple information. Orientation to the proper column was the strength of the approach used. Jeanne Chen [4] extended its functionality by representing the shares in a circular manner to increase the security of the system. The increased choice of angular rotations made predictions difficult. H C Hsu et al [3] also exploited concentric circular areas in the shares for achieving increased capacity. The mechanism involved flipping of shares for decoding of information. However, these techniques performed fairly due to the need of pixel expansion and the use of a code book. Chen et al [16] improved the short comings of these approaches by using random grids to perform the same. The resultant system was efficient and generated restored images with acceptable PSNR values.

Saman et al [10] represented the rectangular shares into a cylindrical manner exploiting the geometric configurations on the shares to decrease the distortion induced in the final resultant information. The paper gave directions for understanding and utilizing the geometrical orientations of the shares for increasing the carrying capacity. Shares can be represented spherically and into cuboids to achieve systems that are secure and have high carrying capacity.

2.3. STEGANOGRAPHY

Steganography makes use of algorithms that embeds secret information with no predictable patterns in the cover and involves use of sufficiently long key to increase security[2]. The identification of the potential region of interest and the embedding efficiency are the main attributes that is used to measure its performance. Payload are transformed to illegible format before embedding to increase security [17].

The Least Significant Bit (LSB) [2] based on spatial domain offers simple mechanisms of embedding the secret. However they have a weak resistance towards statistical attacks. The Pixel Indicator Technique enhances the security of the existing LSB scheme. The LSB of one of the RGB plane is used to specify the presence of data in the other two. The visual distortion is low but the scheme is less resilient towards histogram and visual attacks. Fixed and variable-size LSB embedding techniques have been implemented to improve the performance metrics. Block Matching [9] measures the similarity of the message to be embedded with the carrier for identification of the region of interest. Matrix encoding [24] can be employed to insert the data with minimum distortion. The JSteg algorithm [2] serially embeds data on LSB of non-zero quantized DCT coefficients in a JPEG images with an embedding capacity of over 12%. Frequency based approach are more susceptible to χ^2 -attack. F5 utilizes absolute non-zero coefficients and Outguess [2] uses 0 or 1 coefficients as a platform for data embedding. Steganalysis can detect the existence of data embedded by analyzing the boundary coefficients of blocks (blockiness).

Discrete Wavelet Transformation (DWT) representation of an image into a dyadic wavelet pyramid gives a better representation of time and frequency components. Block partitioning based techniques using DWT [11] have been used to conceal information depending on the texture of the image carriers. Bhattacharya et al. [12] used the diagonal coefficients of DWT sub-bands to hide multiple information. The diagonal DCT coefficients of the sub-bands of individual planes are used for embedding the secret. The volume of data to be embedded and the limited use of diagonal sub bands were the major constraints.

Image realization steganography (IRS) embeds information by taking a cover-to-secret mapping. This decreases the risk of detecting the information by the intruders. Discrete

Wavelet based Steganography [2] have been used to partition the image on the basis of the texture (smooth, edges) to identify potential regions for variable data embedding using image realization.

2.4 HYBRIDIZATION OF VISUAL CRYPTOGRAPHY AND STEGANOGRAPHY

Song et al [25] used the simple LSB matching with Boolean functions for efficiently encrypting and embedding the information on a carrier. Kumar et al [6] embedded the shares generated from traditional visual cryptography scheme into the middle frequencies of an image using DCT. Compression to image quality ratio has been a concern. Roy et al [23] used the inflexion, word order and periphrases in English text for hiding data. The approach lost recognition due to its increased complexity.

3. PROPOSED METHODOLOGY

The proposed system defines a multi-tier security model based on random grids and image realization which can encoded multiple secret information. At the first level, binary images are embedded in concentric circles at various angular displacement in the shares which are represented in a circular fashion. The representation enhances the number of messages which can be embedded and removes the limitation of using fixed angular rotational movements for multiple information mapping. The visual cryptograms can be used for secrecy. Alternatively it also offers a hierarchical approach to validate users in domains where authenticating users is the primary objective. In the second level, the shares generated are concealed in one of the CMY planes of the carrier image by using matrix encoding technique to minimize the distortion on the carrier due to change in pixel information. One of the unused planes is used for indicating the position of the information mapped in the other two planes.

Random grids are generated using Kafri & Keren [7] and are transformed into circular shadows. A completely filled black grid along with a reference grid is utilized for creating circular shares as given in Figure 4.

Fig. 4 Circular Random Grid generation, a) Reference Circle, b) Filled Circle and c) Circular Grid.

The hierarchical tree representation increases the flexibility for implementing authentication functions. Various sector of the circular grids are utilized for increased capacity with the pixel density decreasing as we traverse the share from the inner ring to the outer ring. A basic topology of the hierarchical binary structure is given in Figure 5. The basic 2 by 2 can be extended to 'n' by 'n' scheme using Chen [16] for accommodating increased number of users. As the depth of the tree increases, for each level, concentric regions of the share are explored in an incremental manner fanning from the inner to the outer region as suggested by Jeanne Chen et al [4], where the bandwidth of each region with respect to the depth of the tree is proportional to the width of the secret information. Each level can encode multiple secret information using circular rotations as in Tzung Her Chen [15].

To conceal the shares for storage or distribution, a mapping of the shares is done in one of the non-overlapping blocks of the CMY carrier plane using the standard deviation as a metric for region identification. The share information are then diffused in the potential area of interest using matrix encoding technique [24]. Chaotic scrambling [17] of information can be done before embedding to increase the security of the system. The block size, location and the seed value (optional value needed for Arnold transformation) required for re-transformation can be concealed in one of the carrier planes using Cantor pairing [20] function to decrease the dimensions of the information mapped, which in turn enhances its security.

Fig. 5 Hierarchical representation of the shares (S_i shares)

4. DESIGN

The following section briefly give a schematic overview of the hybrid architecture. The first level of security is focused on implementing the secret sharing scheme using random grids. Accommodation of information is achieved via rotation of shares and exploiting concentric layers of the circular shadows. The noisy patterns are then embedded for distribution using image realization steganography.

4.1. SECRECY AND AUTHENTICATION

The system firstly generates shadows using a 2 by 2 secret scheme. The innermost layer is utilized to hide the information which can also be used as an attribute for authenticating users by assigning one of the shadows generated as a *Master share*. The other share is used as a reference to generate shares for the next level in the hierarchy. For the purpose the next adjacent ring traversed outwards from the inner ring is utilized. For encrypting 'm' secret information on the same shares, each of the secret data are encoded at a distance of (w/m) {where w = width of secret image, m = the number of secret information} in the share. The scheme generates only 2 shares per iteration. To generalize the scheme for 'n' users, the following policy is implemented. The scheme generates 'n' shares with the black and white pixels randomly and uniformly distributed in each of the shares. For the occurrence of a black pixel in the secret image the pixel in the same position in one of the 'n' share is made to 1 while the others are made as 0. On the contrary, for the incidence of a white pixel, the algorithm generates a pseudo random that decides the whether the pixel value of one of the shares chosen randomly is 1 or 0. The algorithm for the proposed visual cryptography is given in algorithm 1.

Algorithm 1: Hierarchical data hiding

Input : Secret Image S_i where $1 \leq i \leq m$

Output: Random Grid $RG_1 \dots RG_n$

```

1. //Generate 'n' RGx random grid
   1.1      for(1 ≤ i ≤ rows and 1 ≤ j ≤ column)
       1.1.1      RGx [i, j] = rand_pixel(0, 1)
2. // Extension : Generation of 'n' by 'n' scheme,
   for (each pixels of secret S[i, j])
   2.1      if(S[i, j] == 1)
       // Choose a random grid
       y = rand_number(n)
   2.2      // Assign pixel at RGy [i, j] as 1, assign others as 0
       RGy[i, j] = 1 & RGx[i, j] = 0  ∀ x ≠ y
   2.3      else
       // Choose a random grid
       x = rand_number(n) , w = random(0/1)
       1 if w ==1,
       RGx[i, j]= 0 otherwise
3. // Hierarchical Construct : depth of the tree 'u'
   for(1 ≤ s ≤ u)
   // Multiple information hiding: RGx as a master grid for storing 'm' secrets
   3.1      for ( 1 ≤ k ≤ m ) do
       for( 1 ≤ i ≤ rows and 1 ≤ j ≤ column) do
       3.1.1      // Shifting of columns
           jnew = j + (k-1)*rows/m
           jnew = jnew % rows
       3.2      RGsx [i, j] = Random_Grid_Generator(RGsx[i + rows, j], Sk [i, j])
4. End

```

4.2. IMAGE REALIZATION STEGANOGRAPHY

The noisy patterns/shares generated at the previous level are embedded by using image realization steganography. A brief outline of the various phases involved in covert writing are given below.

4.2.1. PHASE A

4.2.1.1. MAP GENERATION: A cover-to-secret mapping is generated by adding the pixel information of secret and cover image. The mapping procedure is as follows:

Algorithm 2:

Step 1: Take any plane C of the carrier.

Step 2: Divide the plane chosen into N non overlapping blocks whose size is identical to the secret information.

Step 3: For i = 1 to N

Calculate mapping matrix M: = C_i + S

where C_i is the block taken into consideration , S is the secret image

End

Step 4: Let C_{min} denote the block with minimum embedding bits.

Step 5: Save the mapping matrix.

4.2.1.2. KEY GENERATION: The reversible key is generated by using Cantor pairing function [20]. The function takes two integers 'a' and 'b' to compute the paired value 'h' and the pairing function P (a, b). $h = P(a, b), P(a, b) = (a+b-2)*(a+b-1)/2 + a$ (1)

The reverse procedure calculates the value 'c' which is utilized to derive the values of 'a' and 'b'.

$$c = \lfloor \sqrt{2h-1}/2 \rfloor$$

$$\Delta c = 1/(2) c(c+1), a = h - \Delta c \text{ and } b = c - a + 2 \quad (2)$$

4.2.1.3. MAP EMBEDDING: The embedding of map is done by identifying the rough and smooth block of the selected plane, based on the standard deviation as given in Algorithm 3. The block having standard deviation greater than mean standard deviation is considered as the rough region and higher number of bits is embedded by changing only one bit as compared to the smoother region of the block.

Algorithm 3:

Step 1: Take any plane C_i from the cover image.

Step 2: Divide the plane chosen into N non overlapping blocks whose size is identical to the secret information.

Step 3: Choose a Block and select 'k' bits from the secret message.

Step 4: P = binary equivalent of S .

Step 5: Let K = length (P).

Step 6: while ($K > 0$)

Select Block (i).

Calculate the standard deviation of the Block (STD).

If STD is low

Embed (7, 3).

Else

Embed (3, 2).

End If

End While

Step 7: Save image I as stego image S' .

Embed(M, N) signifies the embedding of N pixels of secret image in M pixels of the carrier image using the matrix encoding. The generation of the stego image is given in Figure 6.

Fig. 6 Encryption Procedure for the Hybrid System.

4.2.2. PHASE B

4.2.2.1. SECRET EXTRACTION: In the extraction procedure, the key information indicating the region of embedding and the secret size is extracted from one of the unused planes. The information needed for decoding is retrieved using equation 1 and 2 as given in Section 4.2.1.1. The algorithm for information reconstruction is given below.

Algorithm 4:

Step 1: Use the reverse Cantor pairing function to extract the key.

Step 2: Generate the mapping matrix M using the key.

Step 3: Take the unused plane.

Step 4: Divide the stego image S' into N non-overlapping blocks.

Let msg=secret message

Step 5: while (K>0)

 Select Block (i).

 Calculate standard deviation (STD) of the Block.

 If STD is low: Bits=Extract (7, 3).

 msg =append (msg, bits).

 Else

 Extract (3, 2).

 msg =append (msg, bits).

 End If

End while

Step 6: Save the modified image I as stego image S'.

A schematic diagram for the secret information retrieval is given in Figure 7.

Fig. 7 Decryption Procedure for the Hybrid System

5. RESULT AND DISCUSSION

The simulation of the proposed system was implemented on MATLAB 7 (R2010B). The ciphers generated on various different sizes were evaluated on the basis of visual quality, structural similarity and security. The carrier images are evaluated in accordance with the embedding efficiency and their visual quality. The analysis of the authentication visual cryptographic scheme is given in the first part, image realization based steganography is assessed in the second phase and finally the third section discusses the performance analysis of the hybrid system.

5.1. AUTHENTICATION BASED ON RGVCS SCHEME

The proposed scheme can be used for validating shares for group communication so as to avoid cheating of the shares to reveal the secret information. Visual distortion due to embedding of noise is seen on overlapping the shadows and using the Human Visual System to decode it.

Binary images of 280 x 100 pixels was taken as an input. The master secret information “@PP1E” is used for authenticating the users at the first level. Two secrets “TEST” and “CODE” are embedded at the second level at the outer zone of the circular share with one of the master shares generated in level 1 as an input. A maximum of four secrets can be embedded at each level to reconstruct shares with acceptable visible quality. The final results are given in Table I.

Table I. Details of Simulation of an approach for Circular Random Grid with Share Authentication for the Secret Image size 280 x 100 pixels					
Sl No	Method	Initial Image	Grids Generated	Overlapped	Remarks
1	(3,3) RG	@PP1E		@PP1E	<ul style="list-style-type: none"> Generate Master Shares: extension of (2,2) scheme to 3:3. Level 1 authentication
2	Proposed System On shifting of columns	TEST CODE		TEST CODE	<ul style="list-style-type: none"> Use of one of the master share generated in the previous level for the shares to be generated in the next level. Level 2 authentication. Multiple secrets hiding with α column shift. Contrast more than 10%.
3	Proposed System With circular representation	@PP1E CODE TEST			<ul style="list-style-type: none"> Circular representation with rings. On α rotation multiple secrets can be revealed. No of Concentric rings can be increased. Multiple secret hiding is easy and flexible. Share Authentication done. Contrast more than 10%

5.1.1. VISUAL QUALITY: The metric measures the effectiveness of the decoded information with respect to contrast and accuracy by comparing the decoded information

with the original one. Accuracy for the reconstructed secret image is estimated by using the peak signal-to- noise ratio (PSNR). Higher values indicate the closeness of the decoded information to the original one.

The contrast 'α' is evaluated as

$$\alpha = L(A(S(0))) - L(A(S(1))) / (1 + L(A(S(1)))) \quad (3)$$

where $L(A(S(0)))$ and $L(A(S(1)))$ refers to the average light transmission of the white and black pixels. For the multiple information hiding scheme [15] the contrast is evaluated as

$$\alpha = 2/(5m-1). \quad (4)$$

PSNR uses the mean squared error (MSE) for measuring the quality of the reconstructed image. The contrast and the PSNR value for the experimental data computed by using equation 3 and 4 are given in Table II. The experimental values are closes to the theoretical value suggested by Tzung [15].

Table II. Contrast and PSNR value for variable secret sharing in image size of 280 x 100 pixels				
		Contrast		
No of Secret Message	Size of Image (pixels)	Theoretical Value	Experimental Value	PSNR
1	280x100	0.50	0.4753	4.512
2	280x100	0.22	0.2287 0.2072	4.3240 4.6266
3	280x100	0.1429	0.1449 0.1427 0.1423	3.8773 3.8198 3.8096

5.1.3. STRUCTURAL SIMILARITY INDEX METRIC (SSIM)

SSIM [2] measures the similarity between two images, the simulated result of a 2:2 scheme is given in Figure 8. It measures the image distortion based under loss of correlation, luminance distortion and contrast distortion. The structural similarity between the two images X and Y of common size $N \times N$ is calculated with different window sizes of the image and is given in equation 5.

$$SSIM(X, Y) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (5)$$

Where μ_x, μ_y denotes the average windows of X and Y. The covariance of X and Y is given by σ_{xy} and σ_x^2, σ_y^2 denotes the variance of X and Y respectively. Constant values $c_1=(k_1l)^2$ and $c_2=(k_2l)^2$, where $k_1=0.01$, $k_2=0.03$ and l is the dynamic length of pixel value with default value 255.

Fig. 8 Structural Similarity (SSIM) analysis between the original image and the shares generated

Share 1 contains a uniform distribution of 0's and 1's. The similarity correlation is minimize for share 2 as the pixel distribution is controlled by the secret information. The negative structural similarity (SSIM) index of the shares generated shows minimal correlation of the shares with respect to the original shares.

5.1.3. SECURITY: The individual shares do not reveal any patterns useful for decoding the final secret information. The contrast for such shares is computed as 0 indicating an equal area of black and white pixel distribution.

The proposed system implements a hierarchical distribution of secret images flexible, simple and easy to manage. The 2 by 2 scheme requires 'n+1' shares to authenticate 'n' users in lieu of $2*n$ share reducing the number of shares and making the system efficient to use. For 'm' concentric rings, a maximum of $(4*m + 1)$ secret data can be hidden.

5.2. IMAGE REALIZATION BASED STEGANOGRAPHY

The proposed algorithm was evaluated for image fidelity and its embedding efficiency.

5.2.1. PEAK-SIGNAL-TO-NOISE RATIO (PSNR) & STRUCTURAL SIMILARITY (SSIM): The quality of stego image is evaluated in terms of Peak-Signal-to-Noise Ratio (PSNR). The results listed out in Table III reflects PSNR value consistently greater than 40 dB greater than the threshold value for visible human distortion. The PSNR comparison of the algorithm suggested with JSteg and LSB is shown graphically in Figure 9.

Fig. 9 PSNR comparative of the proposed system with other standard algorithms

The result shown by the Figure 9 reveals that the proposed method yields PSNR better than JSteg and LSB thus providing better stego-fidelity. The PSNR is also found to be large on secret images of larger sizes.

SSIM is used to check the similarity between the stego and cover image giving a perfect match with the SSIM value as 1. The SSIM for the simulated results are shown in Table III. The Structural Similarity Index is also close to the original image.

Table III: PSNR and SSIM computation					
Cover Image	Secret Image Size	PSNR	Average PSNR	SSIM	Average SSIM
64 x 64	63.6973	62.1188	0.9999	0.9998
	80 x 80	62.2549		0.9998	
	100 x 100	61.2928		0.9998	
	120 x 120	61.2300		0.9997	

5.2.2. EMBEDDING EFFICIENCY: The embedding efficiency gives the ratio between the numbers of secret bits embedded to the number of bits changed in the cover image. The experimental results given in Table IV depicts that for every bit change, the number of bits embedded is at least two.

Table IV: Embedding Efficiency			
Cover Image	Secret Image Size	Embedding Efficiency	Average Embedding Efficiency
64 x 64	2.4347	2.4568
	80 x 80	2.2501	
	100 x 100	2.5712	
	120 x 120	2.5715	

Image Realization based steganography used on the spatial domain offers good embedding efficiency and visual quality for colored secret images. The average PSNR on test data measured to 62.1188. The average structural similarity of the scheme is very close to 1 (0.9998), and the average embedding efficiency computed to 2.4568 bits per pixel.

5.3. HYBRID MODEL

The final output taken from the proposed methodology is reflected in Table V and VI. The rectangular representation is given in Table IV and the circular representation is given in Table V.

6. CONCLUSION

The system provides an effective and efficient way of image secret sharing and distribution. The hierarchical construct provides a flexible architecture which can be easily extended for authenticating multiple users. Exploiting the regions of concentric layers in the shares helps us achieve increased capacity. The number of secrets that can be concealed in a share is proportional to the number of concentric layers. Each layer can store a maximum of 4 secret messages, thus for 'm' number of concentric rings a maximum of $4*(m + 1)$ information can be encoded. The single circular share can also be utilized as single master share with additional 4 number of secret information which is implemented for the root level. The contrast of the recovered images are found to be close to the theoretical value. The noisy shadows are concealed in image carriers which is highly resistant to statistical attacks. The cantor pairing function facilitates in reducing the information of the secret blocks hidden in one of the planes making it difficult to access

the key information for information retrieval. The embedding efficiency of the system using matrix encoding performs fairly with at least two bit of information per every bit change in the cover image. This reduces the distortion induced in the carriers but increases accommodation of the secret bits. The hybrid system can be applicable to wide applications like polling, digital copyright protection, biometrics (iris, fingerprints), digital forensics, etc.

Table IV : Rectangular representation		
Before	After	PSNR
4.3293
3.4959
4.2058

Table V: Circular Representation	
Before	After

REFERENCES

- [1] Adi Shamir, "How to share a secret", Communications of the ACM, Volume 22 Issue 11, Nov. 1979, Pages 612-613, doi :10.1145/359168.359176
- [2] A Cheddad, J Condell, K Curran and P McKeivitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.
- [3] H C Hsu, J Chen, T S Chen, Y H Lin, "Special type of circular visual cryptography for multiple secret hiding", The Imaging Science Journal 55(3), 2007, Pages 175-179.
- [4] Jeanne Chen, Tung-Shou Chen, Hwa-Ching Hsu, Hsiao-Wen Chen, "New visual cryptography system based on circular shadow image and fixed angle segmentation", Journal of Electronic Imaging 14(3), July 2005.
- [5] Jen Beng Feng, Hesien Chu Wu, Chwei Shyong Tsai, "Visual Secret Sharing for multiple secrets", Pattern Recognition 41, Volume 41 Issue 12, December 2008, Pages 3572-3581.
- [6] Jithesh K, A V Senthil Kumar, "Multilayer Information Hiding- A Blend of Steganography and Visual Cryptography", Journal of Theoretical and Applied Information Technology, Vol 19 No 2, 2010, Pages 109-116.
- [7] O Kafri and E Keren, "Encryption of pictures and shapes by Random Grids", Optics Letters Vol. 12, Issue 6, 1987, Pages 377-379.
- [8] M Gnanaguruparan, S Kak, "Recursive Hiding Of Secrets In Visual Cryptography", Cryptologia, vol. 26, 2002, Pages 68-76.

- [9] R Wang, Y Chen, "High Payload Image Steganography Using Two-Way Block Matching", IEEE Signal Processing Letters, 13(3), 2006, Pages 161-164.
- [10] Saman Salehi, M A Balafar, "Visual Multi Secret Sharing by Cylindrical Random Grid", Journal of Information Security and Applications, Volume 19 Issue 3, July 2014, Pages 245-255.
- [11] Suvarna Patel, Gajendra Singh Chandel, "Performance Analysis of Steganography Based on 5 Wavelet Families by 4 Levels-DWT", International Journal of Computer Science and Network Security, Vol 14 No 12, December 2014.
- [12] Tanmay Bhattacharya, Nilanjan Dey, S R Bhadra Chaudhuri, "A Session based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications Volume 38. No 5, January 2012, Pages 18 – 21.
- [13] Tzung-Her Chen, Kai-Hsiang Tsao, "Visual Secret sharing by Random Grids Revisited", Pattern Recognition Volume 42 Issue 9, September 2009, Pages 2203-2217.
- [14] Tsung-Lieh Lin, Shi-Jinn Horng, Kai-Hui Lee, Pei-Ling Chiu, Tzong-Wann Kao, Yuan-Hsin Chen, Ray-Shine Run, Jui-Lin Lai, Rong-Jian Chen, "A novel visual secret sharing scheme for multiple secrets without pixel expansion", Expert Systems with Applications, Volume 37, Issue 12, December 2010, Pages 7858-7869.
- [15] Tzung-Her Chen, Kuang-Che Li, "Multi-image encryption by circular random grids", Information Sciences, Informatics and Computer Science, Intelligent Systems, Applications: An International Journal, Volume 189, April, 2012, Pages 255-265.
- [16] Tzung-Her Chen, Yao-Sheng Lee, Wei-Lun Huang, Justice Su-Tzu Juan, Ying-Yu Chen, Ming-Jheng Li, "Quality-adaptive visual secret sharing by random grids", Original Research Article Journal of Systems and Software, Volume 86, Issue 5, May 2013, Pages 1267-1274.
- [17] V I Arnold, A Avez, "Ergodic Problems in Classical Mechanics", The Mathematical Physics Monograph Series, W A Benjamin, Inc, Preis geb, New York, 1968.
- [18] William Stallings, "Cryptography and Network Security", Seventh Edition, Pearson Education, 2017, ISBN-10: 9789332585225.
- [19] Wu, L. and Chen H. A Study On Visual Cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.
- [20] "Pairing Function", Source: <http://mathworld.wolfram.com>, Last Access: July 2013.
- [21] Joy Jo-Yi Chang and Justie Su-Tzu Juan, "Two secret sharing scheme by Shifting Random Grids", Proceeding of the 29th Workshop on Combinatorial Mathematics and Computation Theory, National Taipei College of Business, Institute of Information and Decision Sciences, Taipei, Taiwan, April 27-28, 2012.
- [22] Naor M., Shamir A. (1995) Visual cryptography. In: De Santis A. (eds) Advances in Cryptology EUROCRYPT 1994. Lecture Notes in Computer Science, Vol 950. Springer, Berlin, Heidelberg.
- [23] Sangita Roy, Manini Manasmita, "A novel approach to format based text steganography", Proceedings of the 2011 International Conference on Communication, Computing & Security, ICCCS 2011, Odisha, India, February 12-14, 2011.
- [24] Shabnam Samima, Ratnakirti Roy, Suvamoy Changder, "Secure Key Based Image Realization Steganography", 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), December 2013, Publisher : IEEE Xplore.
- [25] Shouchao Song, Jie Zhang, Xin Liao, Jiao Du, Qiaoyan Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advanced In Control Engineering and Information Science, Procedia Engineering 15 (2011) , Page no : 2767-2772.