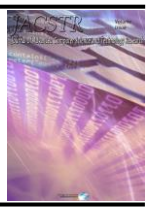

Enhancing Shamir's Secret Sharing Using Gaussian Elimination Based on Hybrid Transform (Integer WT-DCT)

Salah S. Mustafa[1], Ahmed S. Fasih[1], Ahmed T. Sadiq[2]

[1] Computer Science Dep.-IT & CS College- Al-Anbar University, Al-Anbar, Iraq

[2]Computer Science Dep.- University of Technology, Baghdad, Iraq

drahmaed_tark@yahoo.com

ISSN: 2231-8852

ABSTRACT

A secret sharing is an important tool to share the secret key among N users in a secure manner with the need to treat the main problems of increment shares volume and sharing control. Based on the hybrid transformations, a new technique of sharing scheme with excellent sharing-control flexibility is suggested to share a secret image into multiple shadow pictures (for N users) utilizing a scheme of Shamir's threshold beside a method for solving a system of linear equations by Gaussian Elimination to remade the secret. This scheme applied a hybrid I-WT and DCT firstly to de-correlate image pixels for more reduction in image size; then it employs the modifying Shamir's (k, n) sharing scheme to generate the shadow images. A quality refinement of the recouped picture is accomplished by the information collected from the threshold (k) of share images, and each of one has no data about the secret image. The shadow image size for everyone is smaller than [1/3.5*(v / k- 0.1)] of the secret image (where v=2,3,.., according to k value) and any number of shadow pictures that is not as much as k or larger uncovers no data about the secret. This technique is secure for image sharing with excellent time execution and gives fantastic (PSNR) value rate [greater than 34 db] as shown in result table using integer WT and DPCM that keeps an image quality good, however, much is still expected.

Keywords: Secret Image Sharing (SIS), Integer Wavelet Transform (I-WT), Discrete Cosine Transform (DCT), RC4, RLC, DPCM, Gaussian Elimination (GE).

1. Introduction

Information security turns into an essential issue these days. In a certain application, it is a hazard if an arrangement of mystery information is held by just a single individual without additional duplicates because the secret information might be lost or adjusted. In many different cases, it may be important for a group of people to share a specific arrangement of mystery information. Transmission or storing secret data, for example, business writings, military mystery, and private medical picture, etc. is an exceptionally unique and handy issue (Huang & Li, 2007).

Secret sharing (SS) indicate a strategy for circulating secret among a group of members, each of whom is given a share of the secret information. This secret can be recovered just when an adequate number of shares are collected together; singular shares are of no utilization all alone (Shamir, 1979).

In this Era, where sharing of an image has turned out to be fundamental and is a piece of the clear majority of the exercises being performed on the web. Secret Image Sharing (SIS) is one of the most important types of secret sharing, which was proposed firstly by Shamir in 1979. SIS keeps the Secret Picture X in safe side (away from attackers) by disseminating parts of the picture data (called shares) to an arrangement of members so that, all approved people together can reconstruct the image X' with the end goal that, X and X' are optically indistinguishable.

This paper introduces a new technique of secret sharing for a color image by modifying Shamir's SS approach using Gaussian Elimination based on hybrid transform (DCT & IWT) (Burden & Douglas, 2010). This new approach satisfies low sharing size, more security with a good result at a time, in recovering image quality (PSNR). The other important thing which provides control flexibility in sharing size with PSNR using RLC factor (x) (increase RLC factor Leads to, decrease sharing size and then PSNR and vice versa).

The remaining part of this paper is as follows: an explanation of related works in Section 2, Description of secret image sharing in Section 3. Section 4 and 5 presents our proposed system and the general scheme respectively. The Experimental Results & Discussion, as well as the advantages of proposed technique, are examined in Section 6. Finally, we have the conclusion in Section 7.

2. Related Works

Shamir (1997) provided the first polynomial based secret sharing scheme, it is known as Shamir's secret sharing scheme. Later, Shamir’s approach is applied on images to share it in a secure manner. It depends on polynomial to encrypt each pixel in the image as a scalar value (as a secret) into n shares (with same original image size) using mod prime random number (in the range of 2^{8}) and threshold (k) as the degree of this polynomial. The Lagrange Interpolation is reconstructing the secret image sufficiently.

In Thien and Lin (2002), researchers succeeded in improving Shamir's (k, n) threshold scheme of secret image sharing method that distributed secret image among n members, and any k members could coordinate to remake the secret image, while k-1 or fewer members could get nothing. Thien and Lin's technique used the same polynomial to derive n shares but in a different manner. They took k of not-shared pixels (sequentially) from the original image, then put these values as a polynomial coefficient (instead of one pixel in the first coefficient and chosen the others randomly in Shamir approach), and Lagrange is also used in rebuilding the image in recovering phase. It is important to note that, many research about image secret sharing schemes after 2003 depend on frequency domain (instead of the spatial domain before it).

Huang and Li (2007) introduced a technique for image sharing that rely on the reversible integer-to-integer (ITI) wavelet transform which works in the frequency domain. In this method, the data is encoded (either by arithmetic coding or by Huffman coding) after passing

it through a transformation phase; then the compressed data is sent to the sharing phase to split it to (n) shadows. This secret image is recoverable by combining any k ($k \leq n$) of these shadows.

Yang et al. (2011) proposed a fast secret image sharing scheme based on Haar wavelet transform and Shamir's method. They utilized discrete Haar wavelet transform to decrease the secret image to its quarter size (i.e., by reducing 3 of 4 sub-band except for LL). At that point, the adjusted Shamir's approach is connected just on this LL sub-band to create shadows.

Ashwaq and Loay (2013) has proposed a visual cryptography technique which has been applied to a colored image to perform secret sharing threshold (k, n) based on wavelet. In this framework, a compression of the image was adjusted to decrease the image size for efficient transmission and storage of secret images, while a random generation function and a linear system have been utilized in the construction of secret image sharing scheme. The method described in Ashwaq and Loay (2013) was used with DCT transform as well as some modifications to construct a system for sharing the secret gray image (Ashwaq and Loay, 2014).

Kuang (2013) proposed (k, n) threshold secret image sharing scheme used on light images with low overhead data. A secret image is encoded into n noise like shadow image to satisfy the condition that no information about secret can be uncovered from any k-1 or lesser shares. The size of shares is little. The real contrast between this technique and the strategy of Thien and Li (2002) was that a prime number 257 had been utilized which has removed the truncation error, but numerous details remain crucial.

Koikara et al. (2015) proposed a scheme that uses Shamir's scheme by sharing images in cover images that have been transformed to the frequency domain using block-DCT

Cuicui et al. (2014) proposed a useful method of recreating the distributed <k, n> threshold secret sharing scheme based on spherical coordinates & TAN's scheme. They used Gaussian elimination method to calculate four points to remake the sphere center. It has achieved an acceptable result in computation complexity & storage space.

3. Secret Image Sharing (SIS)

The idea of a secret sharing scheme (or can be indicated as threshold scheme) to take care of the main fundamental issue (secret key used to encode and unscramble) was initially presented independently by Blackley (1979) and Shamir (1979). The (k, n) threshold approach is intended to split the single main key to (n) distinctive shadows. So, the shared mystery is reversible from any k ($k \leq n$) shadows and obtains of k-1or lesser shares gave no data about the secret. More formally, in a secret sharing, there is one manager (dealer) and n participants. The manager gives a secret after converting it to another form by sharing algorithm to the participants in the system, just when share condition is satisfied. The merchant finishes this by giving every player a partake in a manner that any gathering of k (for threshold coefficient) or more players can together recreate the secret, but no gathering of less than (k) players will be able to reconstruct it. Such a system is called a (k, n)-threshold scheme, which is considered one of the basic methods in secret sharing (the other called Visual Cryptography SS).

Secret image (SI) is a common and one of the most important types of secret sharing which is the technique and science about the assurance of essential pictures by circulated storages. The essential thought is to change an image into different uninspiring shadow image in a manner that a qualified subset of the shadow images can reproduce the first picture, yet no secret data can be uncovered by a prohibited subset of the shadow pictures. This can also be applied to text, audio, video as shown in figure 1.

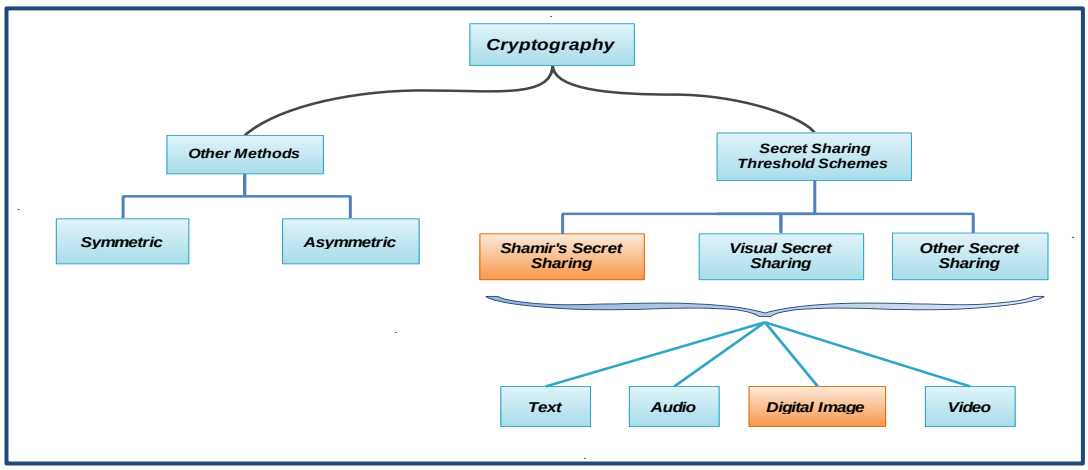

Figure 1: Cryptography Classification

Cryptography system has a common shortcoming, that is the security issue of information storage. Secret sharing strategy is a secure one that can upgrade the security of digitized information. By part, the digitization of information into a few pieces can diminish the dangers of data corruption.

Noticeable, a perfect Secret Sharing Scheme must fulfill high security, great exactness, low computational unpredictability, and no pixel extension. All schemes must fulfill the security condition, and many of the schemes can reproduce the secret image precisely

4. The Proposed System

The principal challenge confronting secure secret image sharing assignments are an increment of sharing volume and control adaptability. Albeit, few works have been devoted to concentrating on the issue of imparting secret shading image to focus on diminishing the shared measure. Still, there is need to do more to decrease the size of the share. In this paper, a new scheme based on hybrid transform coding is produced to make packed SIS in the case when the secret image is a colored one. Figure 2 illustrates the structure of the proposed system.

The main principle of the proposed work on color image is on space and data transfer capacity required in contrasted with binary images or grayscale. Since reducing the color image size is essential for effective storage and transmission, the main outline of the proposed approach in this paper was focused on:

4.1 Modify Run-Length Coding (RLC)

It is an easy way to represent symbols efficiently and competently. If the symbols in a series of successive symbols in a signal are the same, then the symbols will be replaced with one symbol plus the length of the run of that symbol.

This paper introduces a modification by adding a parameter (X) which represents the number of values range (from zero to its factor) that became zero after applying inverse RLC instead of encoding just zeros in the basic method. This led to making it a lossy of entropy coding. An example, when X=5 this means that the values from (0-5) become zeros. The suitable range for this factor is between (5 - 40) according to the experiment. The modification makes the RLC algorithm more flexible with the acceptable losing of data in the recommended range.

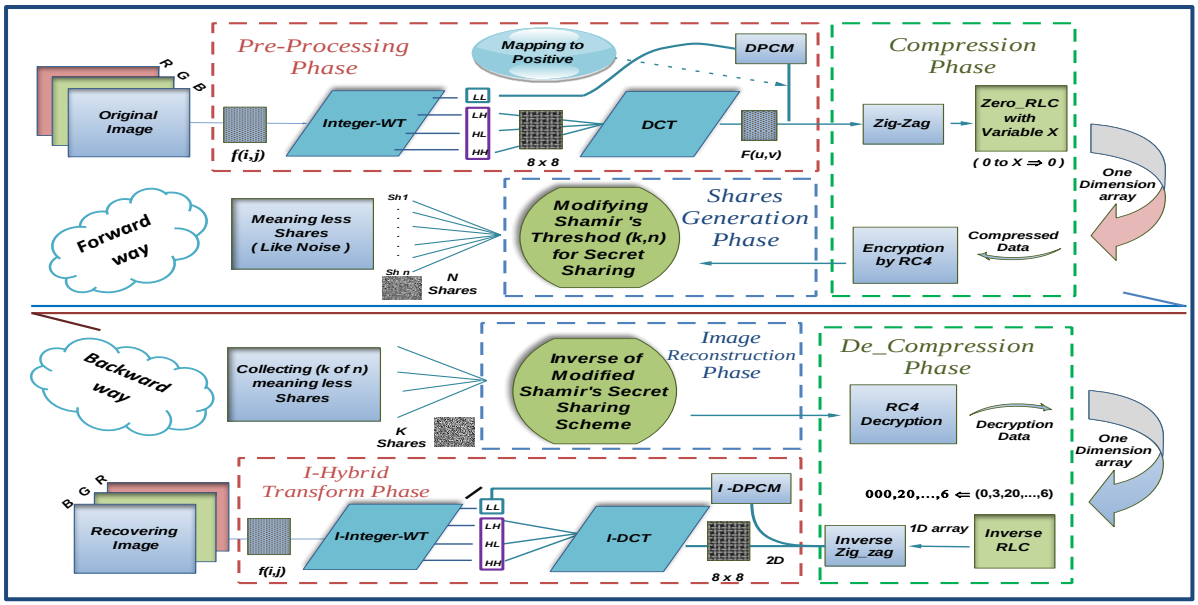

Figure 2: Proposed System Structure

Example :

If X =7 & series of *data is*: 21,95,**0,0,0**,2,0,0,4,1,0,0,11,-10, -5,0,0,5,0,8.

Then R-Length Compression: 21,95,**0,10**,11,-10,-5,**0,4**,8.

R-Length De-Compression: 21,95,**0,0,0,0,0,0,0,0,0,0**,11,-10, -5,**0,0,0,0**,8.

4.2 Proposed Secret Image Sharing Method

Many researchers focus on developing Shamir's algorithm because of its basic model of secret sharing (Thien and Lin, 2002; Yang et al., 2011). They try to make share size and the time of generation small as much as possible with a high level of security and ensuring the quality of recovered image is acceptable.

This paper tries to achieve the desired results in secret sharing field using modified Shamir's algorithm based on hybrid transformation & linear equations to recreate the secret.

4.2.1 Generate Shares

Assuming that we need to share a secret image (SI) into n shadows (SI_1,…., SI_n). The proposed approach used polynomials like Shamir to create these shares but without random coefficients and *mod* operation. There are some things in Shamir (1979) that are used here:

1. The proposed way depends on threshold sharing (k, n), this means k out of n shares where **k** represents the qualified number of (n) shares used to reconstruct a secret.
2. While k-1 or fewer (of n created shares) could get nothing.

The proposed sharing method is listed in the following steps:

1. Divide an image into non-overlapping blocks involve **k** pixels, each one is used to build a polynomial to create a shadow image. It means that all coefficients of the polynomial equation ($a_0,\ldots,a_{k-1}$) are pixels values that generate the (k-1) degree polynomial instead of just one secret in a_0 for traditional Shamir's scheme as described in Shamir (1979) and Chaudhuri (2013).
2. Take a first block of image & use its pixels' values as polynomial factors ($a_0, \ldots, a_{k-1}$) in eq. (1):
   $$F(x) = a_0 + a_1X^1 + a2X^2 + - - - + ak\text{-}1\ X^{k-1} \quad where \quad X=1,2,\ldots.n. \quad \ldots\ (1).$$
3. Substitute the *X* value in eq. (1) which represent here the (*IDs*) of *n* participants, to form new values by calculating the following:
   $$SI_1=F(1)\ ,\ SI_i = F(i),\ \ldots..\ ,\ SI_n = F(n) \quad where\ i=1,2,\ldots,\ n\ . \quad \ldots\ (2)$$
4. Repeat the steps from 2 to 3 for all image blocks until all pixels are processed.

The new ***n*** output values for each block acts as pixels which are distributed sequentially to the n shares. So, each block ***i*** gives one of the generated pixels to every ***n*** shadow images.

The most important thing here is that these new values from the polynomial are formed without using any prime mod number because the proposed approach used a linear method (Gaussian Elimination) to retrieve the original image. This is a big problem because of the limitation of image values in the range (0-255); while the polynomial produces large numbers when a ***mod*** operation is ignored. This paper introduces a solution by doubling (pixel expansion) the image size. Multiplied by 2 for k ≤ 4, because of the need for two levels to distribute the pixels values on it while it is multiplied by 3, 4,.., for >4. These are done to enable this algorithm store these values within the image without losing, using the division and the rest of the division by (256) shown in figure 3.

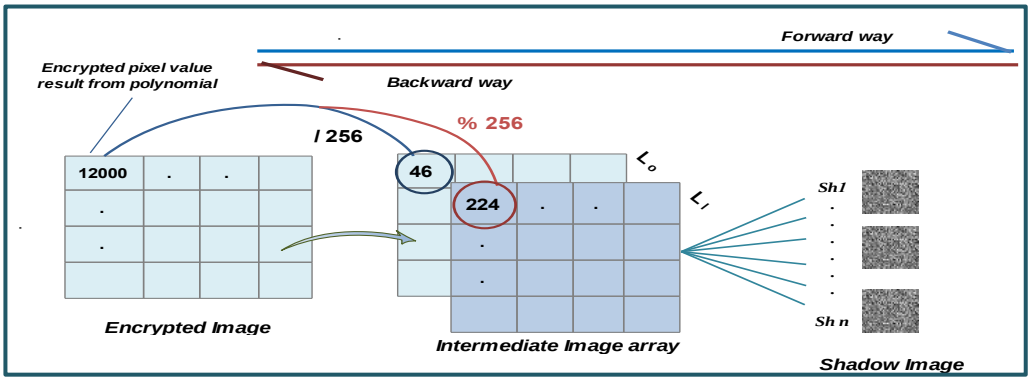

Figure 3: The Expansion of an image size before sharing phase

Notes that the size of each share (in fig.3) becomes nearly to [2*Size $_{\text{Original Image}}$ /k- 0.1].

4.2.2 The Recovering Phase

In this phase, the secret image can be obtained utilizing any ***k*** or larger of shares to retrieve it. Shamir used a Lagrange Interpolation in decoding an image with a ***mod*** operation which is the limit and was not able to restore all encrypted pixels in this case; So, the suggested approach replaced the classical way with a linear equation that utilizes matrices & Gaussian Elimination method to extract the original pixels. The following steps are the proposed for reconstructing a secret sharing approach:

1. Collecting any ***k*** of ***n*** participants' shares, then select the non-used pixels one by one from each of these *k* share images and rearrange them sequentially to form the intermediate image array until all these pixels are handled.
2. Use the multiplication (by 256) for $level_0$ plus $level_1$ (for k<=4) sequentially for each element in the intermediate array to obtain an encryption image that has elements with large number value (*See figure-3 in feed backward way*).
3. Take ***k*** encrypted pixels with participants' *ID* at a time to build a matrix which is used as input into *Gaussian Elimination* function (explained later) to solve for the coefficients (a_0 - a_{k-1}) in Eq. (1). These coefficients are then the corresponding ***k*** pixel values of a secret image.
4. Repeat process 3 until all pixels are handled, and the secret image is recovered.

From Eq.1 adapted from Burden and Douglas (2010), we used the following relations to build a set of linear equations for each temporary block of bytes (created by combining **k** bytes from each of collected shares sequentially to extract the **a's** coefficients which represent a block in recovered image and so on), where $1 \leq i \leq n$, & (***j***) is the number of block, (X_i) is the ID of participants:

$$F(x_i)_j = a_0 + a_1 + a_2 + - - - + a_{k-1}. \quad \rightarrow for\ x_i = 1$$
$$F(x_i)_j = a_0 + 3\,a_1 + 9\,a_2 + - - - +(3)^{k-1}a_{k-1}. \quad \rightarrow for\ x_i = 3.$$
$$F(x_i)_j = a_0 + n.a_1 + n^2.a_2 + - - - +(n)^{k-1}a_{k-1}. \quad \rightarrow for\ x_i = n.$$

This lead to converting these equations into [A]*(x) = [b] matrix form as follows**:**

$$\begin{bmatrix} 1 & 1 & 1 & . & . & 1 \\ 1 & 2 & 4 & . & . & 2^{k-1} \\ . & . & . & . & . & . \\ 1 & X_i & X_i^{\,2} & . & . & X_i^{\,k-1} \end{bmatrix} * \begin{bmatrix} a_0 \\ a_1 \\ . \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} f(1)_j \\ f(2)_j \\ . \\ f(X_i)_j \end{bmatrix} \quad \ldots.(3)$$

The matrices in Eq. (3) can be solved by Gaussian Elimination which will be the main tool of recovering shares technique (Burden and Douglas, 2010). The Gaussian elimination is an efficient algorithm for solving systems of linear equations to allocates the coefficients (a_0 - a_{k-1}) for each collected block and then recovering the secret image.

The Gaussian Elimination algorithm is used to transform a matrix into an upper triangular matrix, called an echelon form matrix. When the greater part of the main coefficients (the furthest left non-zero section in every line) are 1, and each segment containing a main coefficient has zeros somewhere else, then the matrix is in reduced row echelon form. This format uses a succession of elementary row operations to adjust the matrix until the lower

left-hand corner of the grid is loaded with zeros. There are three kinds of elementary row operations:

1) Swapping between two matrix lines, ***2)*** Adding various matrix lines to another, ***3)*** Multiplying a line by a non-zero number.

5. The General Scheme

The general scheme of the proposed color SIS has two parts, the ***Forward module,*** and the ***Backward module***. The Forward module consists of three phases:

(i) Pre-processing phase which represents a hybrid transform using IWT followed by DPCM [apply on just LL band] then DCT,

(ii) Encoding phase of color image based on zigzag and modified Run Length coding with variable factor to compress a transformed secret image followed by RC4 encryption and

(iii) Shares generation phase to create a shadow for all participant in the system.

While the Backward module also consists of three phases which are (sequentially) shares assembler & image reconstruction phase, decoding of recovering image and inverse hybrid transformation phase (See figure: 4).

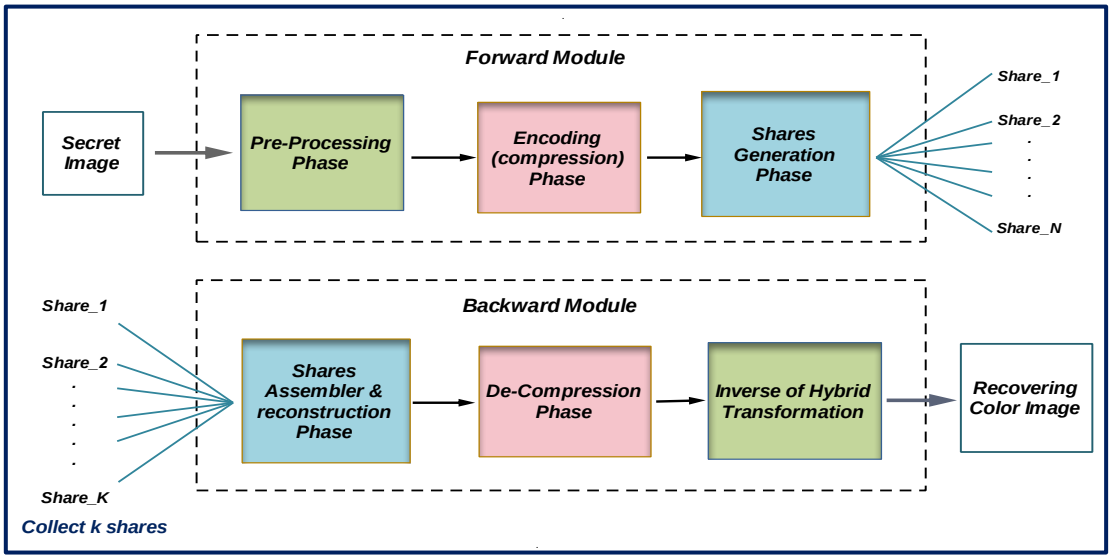

Figure 4: General Scheme for Proposed Color Image Secrete Sharing

The proposed system in designing phase was focused on:

1. The image firstly used as input to **2D-Integer Wavelet Transform (I-WT)** to provide a vast improvement in image quality at high compression ratio mainly. It is utilized to isolate the most valuable information (lowest frequency values) from others to transform data to another format for a more secure system (LL, LH, HL, HH).
2. All wavelet transform outputs (sub-bands: LL, LH, HL, HH) for all components of image color (RGB) are utilized and can't neglect any part, to generate shares with well-recovered image quality as much as possible.

3. The wavelet method split the data into multi-parts for more flexibility control. So, the (LL) sub-band (which is the most important data part) for all color components (R, G, B) are modulated using Differential Pulse Code Modulation (**DPCM**) by determining the differences in adjacent coefficients to save the information quality as a possible:

$$Ai = Ai - Ai\text{-}1, \quad \text{for } i = 2, 3, \ldots, N. \quad \ldots (4)$$

where N is the (LL) length.

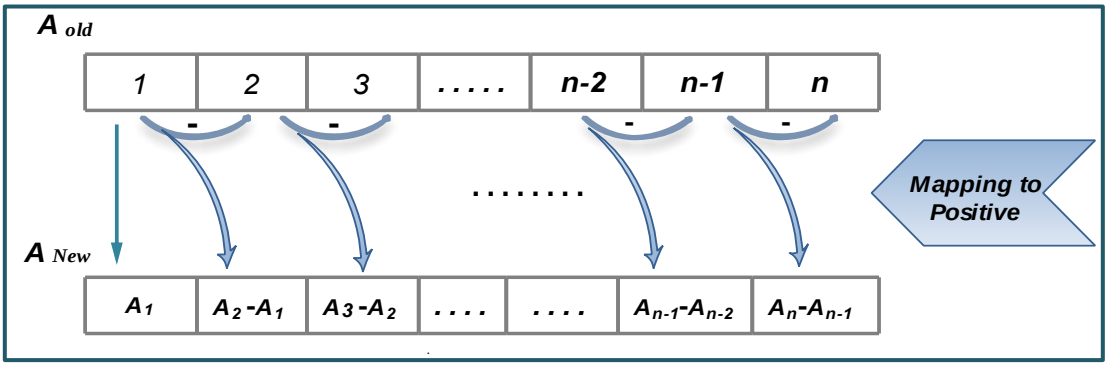

Figure 5: DPCM Technique

Then the DPCM output mapping to positive because it has some negative values, so it must convert to be always positive, by applying the below equation:

$$Xi = \begin{cases} -2x - 1 & if\ Xi < 0,\ \ Xi\ become\ odd. \\ 2X & if\ Xi \geq 0,\ \ Xi\ become\ even. \end{cases} \ldots(5)$$

4. All the other three sub-bands except (LL) pass through Discrete Cosine Transform (***DCT***) method to preserve the principal objectives of improving by reducing shares size (besides using WT), easy maintenance and providing more security. This step achieves the hybrid transform based on (I-WT & DCT as well as DPCM) to provide better compression with an acceptable resolution of recovered images. The steps from (1-4) represent the ***Pre-processing phase***.

5. The technique of **Zig-Zag** scan is applied on DCT output (three of 2D-arrays) in the pre-processing stage to convert them to 1D arrays to exploit the results in the best way, then performing the modified RLC with an insert of X factor value (explained above) to reduce the data. This step makes a good compression (less than **1/3.5** of the original image) for image information because it came after hybrid transform process. The encoding process followed by encryption method is based on the traditional **RC4** which is a fast, simple, efficient & suitable way to ciphering a significant data such as images to make the compressed data more secure. The current step is called ***Compression (Encoding) phase***.

6. The third stage, **shares generation** is considered an important step (which is the backbone of proposed work). The Modified Shamir's threshold of secret sharing is utilized based on traditional polynomials to create shares, and with linear equation by Gaussian Elimination method to reconstruct the original image under Galois Field ($GF2^{8}$) (Shamir, 1979; Chaudhuri, 2013).

Although this adaptive given extension in shares (because it does not use ***mod*** operation in linear equation & the limitation of pixels' value [0-255]) size it is in the acceptable range. Also, it creates shadows and recovering the secret image (from ***k*** out of ***n***) in excellent execution time without losing information (may occur but little according to estimation error) with acceptable shares size which changes based on the value of ***k***:

$$\text{Share size} \approx OI_{size} * 2/k - 0.1, \quad \text{If } k \leq 4, \qquad \text{// where } OI_{size} \text{ is the Original Image Size}$$

$$\text{Share size} \approx OI_{size} * 3/k - 0.1, \quad \text{If } k \leq 8, \text{ when } N \leq k \quad \text{and so on.} \qquad \ldots . (6)$$

The backward module of the proposed system is achieved by performing the following steps:

1. Collecting any ***k*** of ***n*** participants shares and use as input to the first stage of proposed system reverse (***Reconstruction Phase***) that used the inverse of modified Shamir's secret sharing (explained in *section 4.2.2*) to recover the encrypted secret image based on *Gaussian Elimination* instead of Lagrange polynomial to recover all ***a's*** factors.
2. The second stage (De-Compression phase) decrypt the first stage's output by an inverse of the RC4 algorithm with the same key, it is followed by I-RLc (described in *section 4.1*) to decode the compressed information. Finally, the Inverse Zig-Zag (De-scan technique) is applied to recover the original sequence of pixels (as a 2D array).
3. All parts of the output array from the previous stage except the first top left quarter of array (represent the LL sub-band) pass through Inverse-DCT method to obtain the three sub-bands of an image (LH, HL, HH) for all image bands.
4. The LL sub-band (which is not entered to I-DCT) for all color components (R, G, B) are demodulated using Inverse of Differential Pulse Code Modulation (I-DPCM). After performing the mapping to negative (by reverse *eq. 5*) to recovering this part exactly without any missing data using Eq. (7) given below:

$$\boldsymbol{Ai = Ai + Ai\text{-}1,} \quad \text{for } \boldsymbol{i} = 2, 3, \ldots, N. \quad \boldsymbol{\ldots (7),}$$

where ***N*** is the (LL) length.

5. The four subbands are handled as input to inverse integer wavelet transform to rebuild the original secret image with good resolution and recovering time. Note that the last steps (3, 4, 5) represent the third stage (***Inverse Hybrid Transform***) of the backward way of proposed approach, See figure (2 & 4).

6. Experimental Results & Discussion

Various measurements have been carried out to evaluate the performance of the proposed algorithm. PSNR, MSE, and CR defined in eq.(8 - 10) are used as measures to assess the results of this work.

$$\boldsymbol{PSNR} = 10\, log_{10}\, 10\ (255^2)/MSE_{\boldsymbol{RGB}}) \text{ (dB).} \qquad \ldots \textbf{(8)}$$

$$\text{where,} \quad \boldsymbol{MSE}_{\boldsymbol{RGB}} = (MSE_{\boldsymbol{red}} + MSE_{\boldsymbol{green}} + MSE_{\boldsymbol{blue}})/3. \qquad \ldots \textbf{(9)}$$

$$\text{and} \quad \boldsymbol{CR} = Original\ data\ /\ Compression\ data\ . \qquad \ldots \textbf{(10)}$$

Four test color images were used as a secret image (Bear, Children, Flower, Lean). The first three images have the same size (256*256) while the size of Lean is (512*512). See figure6.

Table 1: Proposed System Results based on just Integer-WT

Pic_Name	Original image size (byte)	No. of Shares for (N) Users	No. of (K)	value range (x) with RLC	Size after Com-pression (byte)	CR	Sharing Phase			MSE	PSNR
							Image Dimen. after Sharing	Time of Generating Shares	Time of Shares Recovery		
Bear	(256*256) *3= 196,608	3	2	15	67634	2.90	152*153	00.38	00.32	4.63	41.46
				25	56967	3.45	144*145	00.27	00.35	7.77	39.22
		4	3	20	60938	3.22	144*97	00.23	00.15	6.23	40.17
				30	55460	3.54	136*91	00.27	00.26	8.67	38.74
		5	4	10	86315	2.27	176*89	00.39	00.33	2.48	44.17
				35	54604	3.60	136*69	00.20	00.20	9.36	38.41
Children	(256*256) *3 = 196,608	4	3	15	82327	2.38	168*113	00.20	00.32	5.52	40.70
				30	58563	3.35	144*97	00.32	00.29	12.8	37.02
		5	4	20	69234	2.83	152*77	00.16	00.18	8.48	38.84
				35	56557	3.47	144*73	00.11	00.25	14.35	36.55
Flower	(256*256) *3 = 196,608	4	3	15	64553	3.04	152*102	00.16	00.29	3.58	42.59
				30	55255	3.55	136*91	00.16	00.12	6.55	39.96
		5	4	20	58844	3.34	144*73	00.17	00.19	4.91	41.21
				35	54699	3.59	136*69	00.12	00.19	6.97	39.69
Lena	(512*512) *3 = 786,432	4	3	20	221835	3.54	272*182	00.85	00.37	3.50	42.68
				30	212417	3.70	272*182	00.53	00.34	4.85	41.26
		5	4	35	210847	3.72	272*137	00.33	00.32	5.28	40.90
				40	209992	3.74	272*137	00.31	00.31	5.62	40.63

Table 2: Proposed System Results based on just DCT

Pic_Name	Original image size (byte)	No. of Shares for (N) Users	No. of (K)	value range (x) with RLC	Size after Com-pression (byte)	CR	Sharing Phase			MSE	PSNR
							Image Dimen. after Sharing	Time of Generating Shares	Time of Shares Recovery		
Bear	(256*256) *3= 196,608	3	2	15	98330	1.99	184*185	00.16	00.18	2.32	44.47
				25	83657	2.35	168*169	00.13	00.16	4.59	41.51
		4	3	20	89480	2.19	176*118	00.16	00.14	3.42	42.77
				30	79798	2.46	168*113	00.16	00.13	5.78	40.50
		5	4	10	113841	1.72	200*101	00.18	00.17	1.31	46.93
				35	76962	2.55	168*85	00.13	00.13	6.99	39.68
Children	(256*256) *3 = 196,608	4	3	15	106814	1.84	192*129	00.16	00.17	2.78	43.68
				30	84518	2.32	168*113	00.12	00.13	7.64	39.29
		5	4	20	96946	2.02	184*93	00.16	00.17	4.28	41.80
				35	80427	2.44	168*85	00.13	00.14	9.42	38.38
Flower	(256*256) *3 = 196,608	4	3	15	85887	2.28	176*118	00.15	00.14	0.62	50.20
				30	74849	2.62	160*107	00.11	00.12	3.23	43.0
		5	4	20	82078	2.39	168*85	00.13	00.12	1.30	46.98
				35	72478	2.71	160*81	00.12	00.11	4.20	41.89
Lena	(512*512) *3 = 786,432	4	3	20	315388	2.49	328*219	00.48	00.47	2.15	44.79
				30	291517	2.69	312*209	00.43	00.44	3.60	42.55
		5	4	35	284432	2.76	312*157	00.43	00.40	4.32	41.77
				40	278987	2.81	312*157	00.43	00.39	5.06	41.08

Table 3: The results of Proposed System based on IWT-DCT

Pic_Name	Original image size (byte)	No. of Shares for (N) Users	No. of (K)	value range (x) with RLC	Size after Com-pression (byte)	CR	Proposed Sharing Phase			MSE	PSNR
							Image Dimen. after Sharing	Time of Generating Shares	Time of Shares Recovery		
Bear	(256*256) * 3 = 196,608	3	2	15	55765	3.52	136*145	00.11	00.11	22.67	34.57
				25	53076	3.70	136*137	00.10	00.11	23.36	34.44
		4	3	20	53973	3.64	136*91	00.08	00.11	23.06	34.50
				30	52581	3.73	136*91	00.08	00.09	23.60	34.40
		5	4	10	60219	3.26	144*73	00.09	00.09	22.07	34.69
				35	52308	3.75	136*69	00.08	00.08	23.82	34.36
Children	(256*256) * 3 = 196,608	4	3	15	61255	3.20	144*97	00.10	00.10	19.95	35.13
				30	54839	3.58	136*91	00.08	00.11	21.95	34.71
		5	4	20	57559	3.41	136*73	00.08	00.10	20.89	34.93
				35	54307	3.62	136*69	00.08	00.08	22.19	34.66
Flower	(256*256) * 3 = 196,608	4	3	15	57208	3.43	136*97	00.09	00.09	6.75	39.83
				30	54323	3.61	136*91	00.08	00.08	7.51	39.37
		5	4	20	55461	3.54	136*69	00.11	00.09	7.14	39.59
				35	54140	3.63	136*69	00.08	00.09	7.61	39.31
Lena	(512*512) * 3 = 786,432	4	3	20	215022	3.65	264*182	00.32	00.33	4.74	41.37
				30	211668	3.71	264*182	00.34	00.31	5.15	41.00
		5	4	35	210927	3.72	264*137	00.33	00.32	5.29	40.89
				40	210440	3.73	264*137	00.32	00.31	5.39	40.80

Figure 6: Test Color Images

Tables 1,2 and 3 (T1, T2, and T3) have the same comparing details for three modules sequentially, IWT, DCT and the hybrid. They list the number of bytes before and after compression process with varying (x) values used in RLC, the execution time for creating and recovering shares, and they show some of the objective evaluation parameters: CR, PSNR, MSE.

From these tables, we can see that the number of image bytes in Table 2 for IWT is better than DCT results in compression ratio (CR) because it applies the DPCM on just DCT. Also, the DCT has achieved good results in PSNR & execution time (E.T) comparing with just IWT (appears in Table 1-T1). On the other hand, hybrid technique outperforms these two modules (see Table 3-T3) in general.

Example-1: Use (3, 2) threshold and (x) of RLc is (15), the number of bytes for bear image in ***T2*** for DCT is (98,330 ≈ 184*185 shares size) and PSNR (44.47) when it is (67,634 ≈

152*153 share size) and the PSNR (41.46) in ***T1*** for IWT; while the number of bytes become (55,765 ≈ 136*145 shares size) and the PSNR (34.57) in the same situation at ***T3*** for the proposed system at hybrid transformations.

In general, the new hybrid technique gives us the best result than the other techniques in all measures and these results become perfect in shares size when the number of *K* threshold is equal or less by one with the number of *N* shares, simultaneously with X RLc factor between (30-40) according to experimental tests. Also, note that increasing the X factor larger than 40 decreases the reconstructed image quality and make it not right, but it is also in acceptable range when X between (5-40).

Example-2: In ***T3***, when a scheme is (5, 4) and X value = (40) then Lena image bytes become (210,440 ≈ 264 *137 shares size), MSE= 5.39 and PSNR= 40.80 (See figure-7), and this result is good until it's compared with traditional Shamir's scheme. Also, the execution time is excellent and with good speed technique in both directions (create & rebuild shadows).

7. Conclusions

A perfect system has been proposed which make a good (k, n) secret image sharing module based on hybrid transform using many techniques to decrease the shares size and increase the security as much as possible. It also utilized a good sharing way based on modified Shamir's scheme to share and remake the image pixels through an assembler shares coefficients in each block (have k of values from each share at a time) as a system of linear equations solved by the Gaussian Elimination to reconstruct the secret. It has given us a high reliability to recover an image than other linear systems like Grammar's Rule. The Experimental results affirmed that the proposed technique produces a real reduction in shadow size. As evident during the two steps of compression phase utilizing RLC (smaller than **1/3.5** of its secret image size) and by diminished to (approximately) [**v/k - 0.1**] of a compressed image in sharing phase (where v=2; that represents the amount of the image expansion when k ≤ 4, v=3: k ≤ 8).

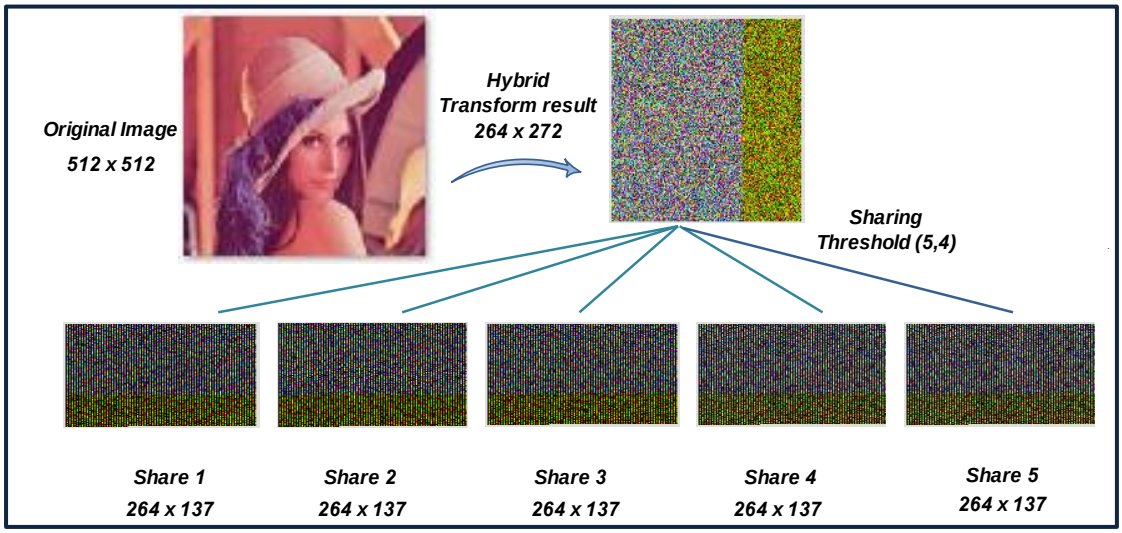

Figure 7: Example of (5, 4) threshold for Sharing process

Also, the table 3 showed that the MSE value of recovered secret image is between (***5.39 & 22.67***) while the value of PSNR measure in the range of (***34.40 - 41.37***). The execution time results were small in both the generation shares and reverse phase; it is in seconds between (***00.08 - 00.34***). The security of proposed structure is ensured by, decorrelation of image transformation utilizing a hybrid (IWT-DCT). The other issue, uncorrelated coefficients become more secure by the standard RC4. Moreover, the last thing is that every share relies upon its appropriate image coefficients, $a_n()$, which made the restoration of the secret excessively confounded for the assailant.

REFERENCES

1- Shamir A. (1979), "*How to Share a Secret*", Communications of the ACM. 11(22), 612-613.
2- Thien, C and Lin J (2002), "*Secret Image Sharing*", Computers & Graphics. (26), 765-770.
3- Huang C. and Li C. (2007), "*A Secret Image Sharing Method Using Integer Wavelet Transform*", Eurasip Journal on Advances in Signal Processing, (2),1-13.
4- Yang C. H., Huang Y. H. and Syue J. H. (2011), "*Reversible Secret Image Sharing based on Shamir's Scheme with Discrete Haar Wavelet Transform*", Electrical and Control Engineering (ICECE), International Conference, Yichang,1250 - 1253.
5- Ashwaq T. Hashim and Loay E. George (2013), "*Secret Image Sharing Based on Wavelet Transform*", International Conference on Information Technology in Signal and Image Processing, Mumbai, India, 324-332.
6- Ashwaq T. Hashim and Loay E. George (2014), "*Secret Image Sharing Based on Discrete Cosine Transform*", International Journal Of Computers & Technology, ISSN: 2277-3061.
7- Kuang S. Wu. (2013), "*A Secret Image Sharing Scheme for Light Images*", EURASIP Journal on Advances in Signal Processing (49).
8- Koikara R., Goswami M., Kim P., Lee G., Yoo K (2015) "*Block-DCT Based Secret Image Sharing over GF (2^8)*", Proceedings of the International Conference on Security and Management (SAM), Computer Engineering and Applied Computing, 2015. p. 178.
9- Cuicui Z., Guangyao W. & Jingwen S. (2014), "*Improved Scheme of Distributed Secret Sharing Based on Personalized Spherical Coordinates Space*", Issue1, pp.5-10.
10- Chaudhuri. (2013),*"Design of A Secured Secret Sharing Technique And Its Application On Mobile Hand Sets"*, M.Sc. thesis, Dept. of Computer Science & Engineering Jadavpur University, Kolkata, May, 2013.
11- Burden L. and Douglas J. (2010), "*Numerical Analysis*", Ninth Edition, Brooks/Cole, Cengage Learning, Canada, 2010.
12- Blackley G. R. (1979), "Safe guarding cryptographic keys," in Proc. National Computer Conference, pp. 313 - 317.