ANALYSIS OF REVERSIBLE WATER MARKING TECHNIQUES AND ASYMMETRIC CRYPTOSYSTEM USING DIEC

Ashlin Rushmi C A[1]
M.E., Electronics and Communication Engineering
Sri Sivasubramaniya Nadar College of Engineering, Chennai

Vinoth Kumar C[2]
Associate Professor, Electronics and Communication Engineering
Sri Sivasubramaniya Nadar College of Engineering, Chennai

ABSTRACT

Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. Whatever type of communication system is in use, it is indispensable to understand the security effects involved. Some essential aspect for secure communications is that of Cryptography and Reversible Watermarking. Here the cover image is embedded with encrypted data by using Difference Pair Expansion Method and is subjected to encryption by using Double Image Encryption Compression technique. Encrypting the image after embedding provides high practical security. On the receiver side the encrypted stego image undergoes the reverse process of embedding and encryption to recover the original image and data. The experimental results showed that our proposed scheme achieved better embedding capacity than the other schemes.

KEYWORDS

Reversible Watermarking, Difference Pair Expansion, Double Image Encryption Compression.

I INTRODUCTION

With this developing world of Internet, it has become extremely needed to the security of data transmission. Maintaining and updating information security in an organization is a challenge. Executing information security in an organization can protect the technology and statistics it uses by preventing, detecting and responding to threats, both internal and external. There are numerous outlook to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. Reversible Watermarking is a technique which enables images to be authenticated and then restored to their original form by taking away the digital watermark and restoring the image data that had been embedded. It would make the images bearable for legal objectives. Thus the cover image is embedded with encrypted data by using Difference Pair Expansion Method and is subjected to encryption by using Double Image Encryption Compression technique.

The prior Reversible Watermarking algorithms are mainly based on lossless compression [10]. Subsequently, Tian proposed the difference-expansion (DE) method [5], a significant spatial domain algorithm which execute on pixel pairs. In Difference Expansion, the secret data is embedded in a reversible way by expanding pixel differences. The correlation between neighbouring pixels are accomplished by DE and a better performance is achieved. Afterwards, Difference Expansion is expanded by Thodi and Rodriguez [7], in which the pixel difference is replaced by the prediction-error

K.S.Babai,P.K.Suresh,K.UmaRani et al. (Eds): ICARTEC-2021
pp. 69 - 82, 2021.IJCI – 2021 DOI:10.5121/ijci.2021.100309

for expansion embedding. Because of the advantages of parallel processing and multidimensional capabilities, [12,16,18], the techniques of optical image encryption have been generally studied in past decades. To enhance the security and enlarge the key space, other domains such as the fractional fourier transform [19], and the gyrator transform [13.14,17,20], are involved in several extensions of the DRPE. To vanquish the security effects inherent in the symmetric system, particular asymmetric cryptosystems have been reported [11,15].

II PROPOSED SYSTEM

The encrypted data is being embedded in the cover image by using Reversible Watermarking algorithm and the stego image is encrypted by using double image encryption compression and the process is shown in Figure 1.

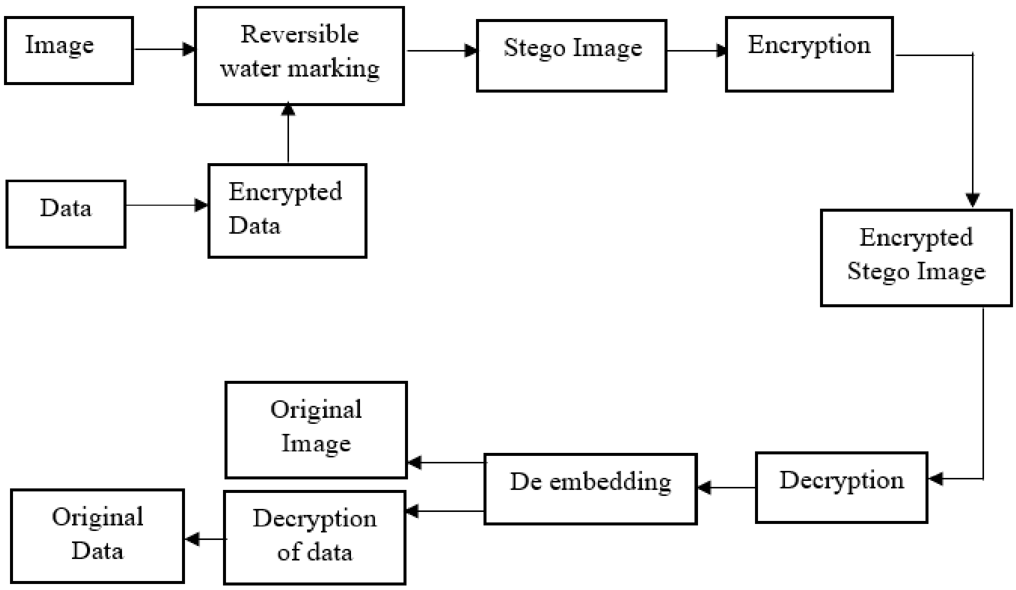


Figure 1: General Block Diagram for the Proposed System

2.1 Data Encryption using AES algorithm

The fundamental prerequisite in security is to hide data from trivial public or malicious attackers. Advanced Encryption Standard (AES) is the most prevalent algorithm used to encrypt and decrypt messages. The schematic of AES encryption is shown in Figure 2.

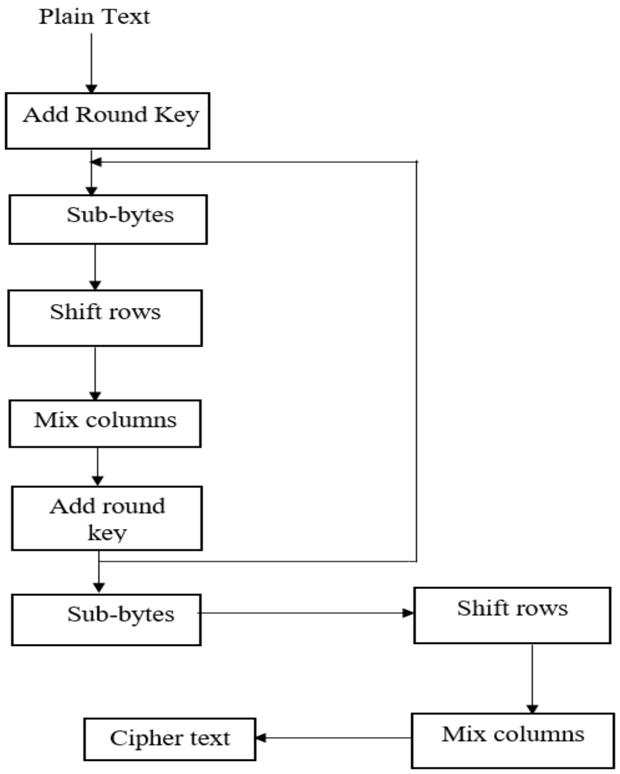


Figure 2: AES Encryption

2.2 Data Embedding using Difference Pair Expansion

First, divide the cover image into non-overlapped pixel-pairs. For each pixel-pair (x, y) compute two difference values d1=x-y and d2=y-z where z is the prediction value of y. Notice that z should be rounded to its nearest integer if it is not an integer. The pixel pairs and the neighbouring pixels are shown in Table 1.

$$z = \begin{cases} v_1 & \text{if } d_v - d_h > 80 \\ (v_1+u)/2 & \text{if } d_v - d_h \in (32,80] \\ (v_1+3u)/4 & \text{if } d_v - d_h \in (8,32] \\ u & \text{if } d_v - d_h \in [-8,8] \\ (v_4+3u)/4 & \text{if } d_v - d_h \in [-32,8) \\ (v_4+u)/2 & \text{if } d_v - d_h \in [-80,-32) \\ v_4 & \text{if } d_v - d_h < -80 \end{cases} \quad (1)$$

where $\{v_1, v_2, \ldots\ldots. v_{10}\}$ are the neighbouring pixels of (x, y).

$$d_v = |v_1 - v_5| + |v_3 - v_7| + |v_4 - v_8| \quad (2)$$

$$d_h = |v_1 - v_2| + |v_3 - v_4| + |v_4 - v_5| \quad (3)$$

$$u = (v_1 + v_4)/2 + (v_3 - v_5)/4 \quad (4)$$

Table 1. Pixel Pair And Neighboring Pixels

	j	j+1	j+2	j+3
i	X	Y	v_1	v_2
i+1	v_3	v_4	v_5	v_6
i+2	v_7	v_8	v_9	v_{10}

The process of embedding of encrypted data is shown in the below Table 2.

Table 2: Process Of Embedding

<table>
<tr><th>Conditions (d_1, d_2)</th><th>Marked value</th></tr>
<tr><td>$d_1 = 1$ and $d_2 > 0$</td><td>(x+b,y)</td></tr>
<tr><td>$d_1 = -1$ and $d_2 < 0$</td><td>(x-b,y)</td></tr>
<tr><td>$d_1 = 0$ and $d_2 \geq 0$</td><td rowspan="2">(x,y+b)</td></tr>
<tr><td>$d_1 < 0$ and $d_2 = 0$</td></tr>
<tr><td>$d_1 = 0$ and $d_2 < 0$</td><td rowspan="3">(x,y-b)</td></tr>
<tr><td>$d_1 > 0$ and $d_2 = 0$</td></tr>
<tr><td>$d_1 = 1$ and $d_2 = -1$</td></tr>
<tr><td>$d_1 > 1$ and $d_2 > 0$</td><td>(x+1,y)</td></tr>
<tr><td>$d_1 < -1$ and $d_2 < 0$</td><td>(x-1,y)</td></tr>
<tr><td>$d_1 < 0$ and $d_2 > 0$</td><td>(x,y+1)</td></tr>
<tr><td>$d_1 > 1$ and $d_2 < 0$</td><td rowspan="2">(x,y-1)</td></tr>
<tr><td>$d_1 = 1$ and $d_2 < -1$</td></tr>
</table>

2.3 Data embedding using Improved PVO based RDH

First, the cover image is divided into non-overlapped equal-sized blocks. Consider only two-pixel values of the host image. The prediction error is e_{max} = x (1)- x (2). Let b (0,1) is a data bit to be embedded. The maximum pixel x (1) is modified to,

$$x'(1) = x(1) + b \quad \text{if} \quad e_{max} = 0 \qquad (5)$$
$$x'(1) = x(1) + b \quad \text{if} \quad e_{max} = 1 \qquad (6)$$
$$x'(1) = x(1) + 1 \quad \text{if} \quad e_{max} > 1 \qquad (7)$$
$$x'(1) = x(1) + 1 \quad \text{if} \quad e_{max} < 1 \qquad (8)$$

The process of embedding in improved PVO based Reversible Watermarking is shown in Figure 3.

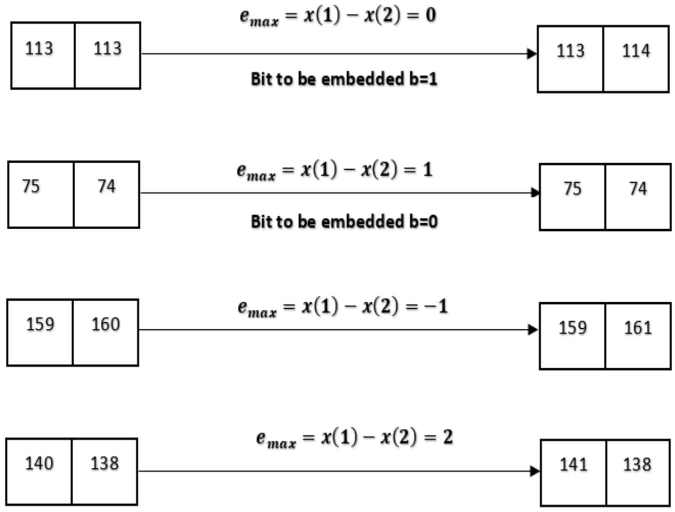


Figure 3: Process of embedding

2.4 Process of Encryption

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. The process of encryption in the proposed methodology is shown in Figure 4.

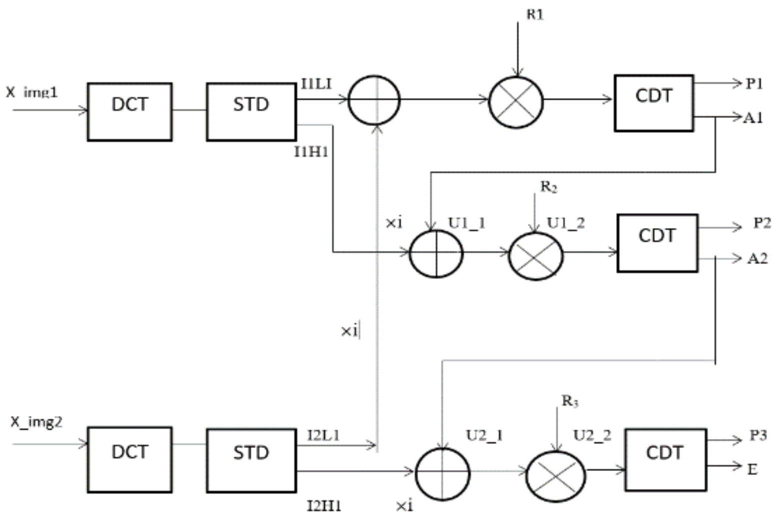


Figure 4: Process of Encryption

2.4.1 Discrete Cosine Transform

The Discrete Cosine Transform (DCT) in Image Processing helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). It is widely used in image compression. The DCT has a strong "energy compaction" property, capable of achieving high quality at high data compression ratios. Discrete Cosine Transform is used in lossy image compression because it has very strong energy compaction, i.e., its large amount of information is stored in very low frequency component of a signal and rest other frequency having very small data which can be stored by using a smaller number of bits (usually, at most 2 or 3 bit). To perform DCT Transformation on an image, first we have to fetch image file information (pixel value in term of integer having range 0 – 255) which we divide in block of 8 X 8 matrix and then we apply discrete cosine transform on that block of data. After applying discrete cosine transform, it can be seen that its more than 90% data will be in lower frequency component. After applying DCT the images get compressed and the spectrum coefficients should udergo scan- then discard (STD).

2.4.2 Zigzag Scanning

The zig-zag scanning pattern for run-length coding of the quantized DCT coefficients was established in the original MPEG standard. The same pattern is used for luminance and for chrominance. A modified (alternate) pattern more suitable for coding of some interlaced picture blocks was added in the MPEG-2 standard. Suppose we have an image of 8 x 8pixel values as shown in Figure.5, then the pixel values are scanned in a zigzag manner as shown in Figure 6.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Figure 5. Pixel values of 8 x 8 image

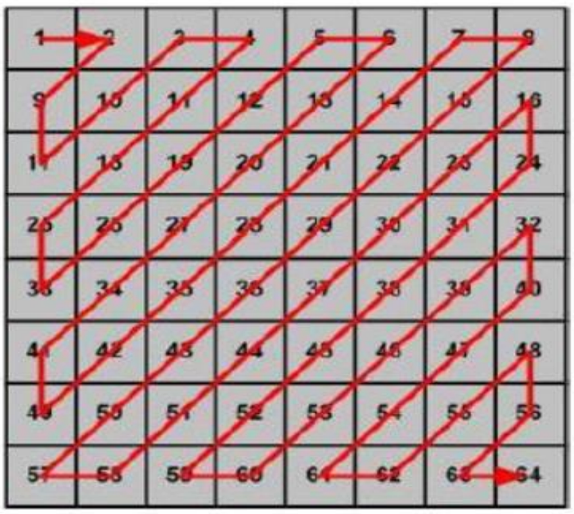


Figure 6. zigzag scanned pixel values

In the proposed encryption process, each plaintext of double images is first converted into spectrum coefficients (SCs) by DCT. The Spectrum Coefficients are zigzag scanned, the first 1/4 of Spectrum Coefficients is resized to two low-frequency images, the second 1/4 of Spectrum Coefficients is resized to two high-frequency images, while the last 1/2 of Spectrum Coefficients is discarded. It is shown in Figure.7.

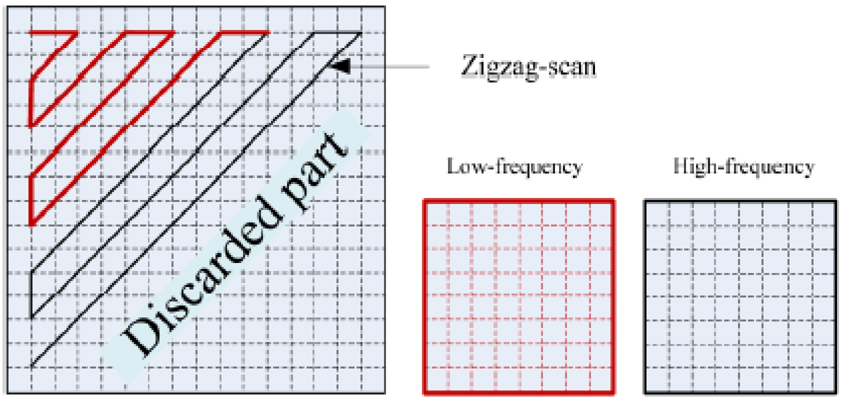


Figure 7. Framework of compression using zigzag-scan-then discard

From the figure, the first 1/4 of spectrum coefficients is denoted as I_1L and the next 1/4 of spectrum coefficients is denoted as I_1H and the remaining 1/2 of the spectrum coefficients are discarded (STD).

2.4.3 Algorithm for Encryption

Step 1: DCT is first applied to two images x_img_1 and x_img_2, from which the ciphertexts to be encrypted. The compression is performed on the zigzag-scanned DCT SCs by discarding the last half of SCs, which is called scan-then-discard (STD). As a result, two low-frequency images and two high-frequency images are obtained, which are denoted as I_1L_1, I_2L_1, I_1H_1, and I_2H_1.

Step 2: I_1L_1 and I_2L_1 are combined into a complex amplitude $U1$ as real and imaginary parts, respectively, which is represented in eqn.9.

$$U_1 = I_1L_1 + i \times I_2L_1 \qquad (9)$$

where i is an imaginary unit.

Step 3: The complex amplitude U_1 is modulated by a random phase mask R_1, and the result is a new complex amplitude U_2, which is represented in eqn.10.

$$U_2 = U_1 \times \exp(i \times R_1) \qquad (10)$$

where R_1 is a random distribution at $[0, 2\pi]$.

Step 4: Then, a private key P_1 and an amplitude A_1 is obtained through the cylindrical diffraction transformation (CDT) with the input of complex amplitude U_2, which is expressed in eqn.11,

$$[P_1\ A_1] = CDT\ (U_2) \qquad (11)$$

Step 5: I_1H_1 and A_1 are used to replace I_1L_1 and I_2L_1 as inputs, respectively in step 2. A_1 and I_1H_1 are combined into a complex amplitude U_{1_1} as real and imaginary parts, respectively, which is represented as eqn.12.

$$U_{1\_1} = I_1H_1 + i \times A_1 \qquad (12)$$

Step 6: R_1 in step 3 is replaced with R_2 to get another complex amplitude U_{2_1} shown in eqn.9. R_2 has a uniform probability distribution on the interval $[0, 2\pi]$.

$$U_{2\_1} = U_{1\_1} \times \exp(i \times R_2) \qquad (13)$$

Step 7: Then, a private key P_2 and an amplitude A_2 is obtained through the cylindrical diffraction transformation (CDT) with the input of complex amplitude U_{2_1}, which is expressed as eqn.10.

$$[P_2\ A_2] = CDT\ (U_{2\_1}) \qquad (14)$$

Step 8: I_2H_1 and A_2 are used to replace I_1L_1 and I_2L_1 as inputs, respectively in step 2. A_2 and I_2H_1 are combined into a complex amplitude U_{1_2} as real and imaginary parts, respectively, which is represented as eqn.15.

$$U_{1\_2} = I_2H_1 + i \times A_2 \qquad (15)$$

Step 9: R_1 in step 3 is replaced with R_3 to get another complex amplitude U_{2_2} as shown in eqn.16. R_3 has a uniform probability distribution on the interval $[0, 2\pi]$.

$$U_{2\_2} = U_{1\_2} \times \exp(i \times R_3) \qquad (16)$$

Step 10: Then, a private key P_3 and an amplitude E is obtained through the cylindrical diffraction transformation (CDT) with the input of complex amplitude U_{2_2}, which is expressed in eqn.17.

$$[P_3\ E] = CDT\ (U_{2\_2}) \qquad (17)$$

The phases P_1, P_2, and P_3 obtained in the above steps are taken as the private keys, and E is taken as the final ciphertext.

2.4.4 Process of Decryption

The conversion of encrypted data into its original form is called Decryption. Decryption is generally a reverse process of encryption. It decodes the encrypted data or information such that an authorized user can only decrypt the data or information because decryption requires a secret key or password. In the proposed methodology, the private keys P_1, P_2, P_3 obtained from the encryption is used as secret key or password. The process of decryption or the reverse process of encryption is shown in Figure 8.

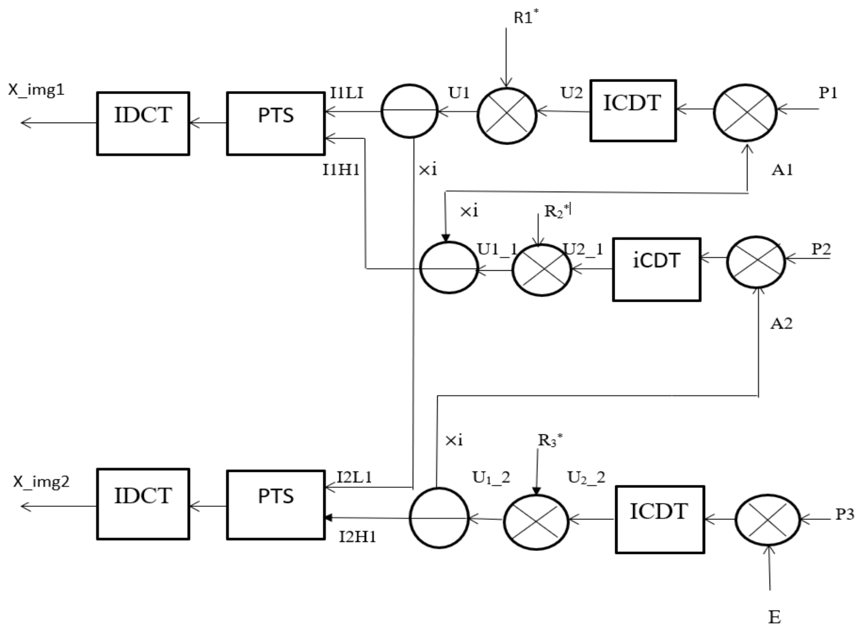


Figure 8. Process of Decryption

2.5 Data Extraction and Image Recovery

2.5.1 Data Extraction of DPM Method

The image obtained after decryption was subjected to de-embedding to extract the embedded data and to reconstruct the original image. The process of deembedding is shown in the TABLE 3.

2.5.2 Data Extraction of Improved PVO based RDH

The image obtained after decryption was subjected to de-embedding to extract the embedded data and to reconstruct the original image. Consider only two pixel values of the decrypted image. The prediction error is e_{max} = x (1)- x (2). Let b (0,1) is a data bit to be extracted. The maximum pixel x (1) is modified to,

$$x(1) = x'(1) - (e_{max} - 1) \quad (14)$$
$$b = e_{max} - 1 \quad \text{if } e_{max} € [1, 2] \quad (15)$$
$$x(1) = x'(1) + e_{max} \quad (16)$$
$$b = -e_{max} \quad \text{if } e_{max} € [0, -1] \quad (17)$$
$$x(1) = x'(1) - 1 \quad \text{if } -1 < emax < 2 \quad (18)$$

The data extraction and image recovery process of Improved PVO based Reversible Watermarking is shown in Figure 9.

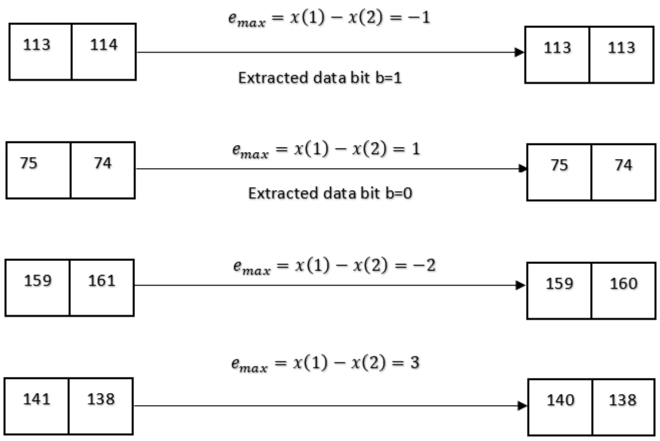
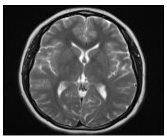
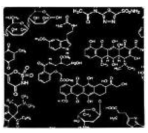


Figure 9. Process of Extraction of data and image


MRI Brain


Heart


CT-Liver


Molecular

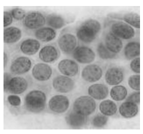

Celulas

Figure 10. Test Images

Table 3. Process of De-Embedding and Extraction of Data

Conditions on (d_1^m,d_2^m)	**Extracted data bit b**	**Recovered value**
d_1^m €{1,2} and $d_2^m > 0$	d_1^m -1	(x^m –b,y^m)
d_1^m €{1,2} and $d_2^m > 0$	-1- d_1^m	(x^m +b,y^m)
($d_1^m = 0$ and $d_2^m \geq 0$) or ($d_1^m = 0$ and $d_2^m \geq 0$)	- d_1^m	(x^m ,y^m–b)
($d_1^m < 0$ and $d_2^m = 0$) or ($d_1^m < -1$ and $d_2^m = 1$)	d_2^m	
($d_1^m = 0$ and $d_2^m < 0$) or ($d_1^m = 1$ and $d_2^m <- 1$)	d_1^m	(x^m ,y^m+b)
($d_1^m > 0$ and $d_2^m = 0$) or ($d_1^m > 1$ and $d_2^m =- 1$)	- d_2^m	
($d_1^m = 1$ and $d_2^m =-1$) or ($d_1^m = 2$ and $d_2^m = -2$)	d_1^m -1	
$d_1^m >2$ and $d_2^m > 0$	No embedded data bit	(x^m –1,y^m)
$d_1^m < -2$ and $d_2^m < 0$	No embedded data bit	(x^m +1,y^m)
$d_1^m < -1$ and $d_2^m >1$	No embedded data bit	(x^m ,y^m–1)
$d_1^m > 2$ and $d_2^m < -1$	No embedded data bit	(x^m ,y^m+1)
$d_1^m = 2$ and $d_2^m < -2$	No embedded data bit	

III RESULTS AND DISCUSSION

The performance analysis of the Reversible Watermarking technique and the experimental results are discussed in this section. The test images taken for calculating performance metrices are shown in Fig 10. The performance metrics used for the reversible data hiding technique are Peak Signal to Noise Ratio (PSNR), Embedding capacity (EC), Mean Square Error (MSE), and Structural Similarity Index Measure (SSIM). PSNR is most commonly used to measure the quality of reconstructed image. The PSNR represents the measure of peak error. MSE measures the average squared difference between the stego image and the original image. The lower the value of the MSE the lower is the error. SSIM is used for measuring the similarity between two images.

Mean Square Error (MSE)

$$MSE = \frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}\big(x(i,j) - y(i,j)\big)^2 \qquad (19)$$

where x *(i, j)* is input image and y *(i, j)* is decrypted image.

Peak Signal to Noise Ratio (PSNR)

$$PSNR = 10log_{10}\frac{255^2}{MSE} \qquad (20)$$

Structural Similarity Index Measure (SSIM) $$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x{}^2 + \sigma_y{}^2 + c_2)} \qquad (21)$$

where μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y, σ_{xy} is the covariance of x and y, $c_1 = (k_1L)^2$ and $c_2=(k_2L)^2$, L is the dynamic range of the pixel-values (typically 255), $k_1 = 0.01$ and $k_2 = 0.03$ (by default).

The performance metrics calculated for various images are shown in the Table 4 and Table 5.

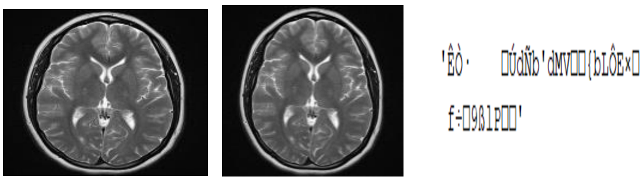
Table 4. Results of Improved PVO Based RDH

Test Image	MSE	PSNR (dB)	SSIM	EC
Brain	0.4172	51.9275	0.9806	8704
Heart	0.3769	52.3686	0.6503	15616
Liver	0.3456	52.7453	0.6320	16768
Molecular	0.3924	52.1936	0.9357	13440
Celulas	0.4231	51.8659	0.9035	11648

Table 5. Results of DPM Method

Test Image	MSE	PSNR (dB)	SSIM	EC
Brain	0.0575	60.5368	0.9995	1408
Heart	0.0148	66.4279	0.9303	2048
Liver	0.0444	61.6537	0.9981	6016
Molecular	0.0431	61.3545	0.9999	3968
Celulas	0.0378	62.3616	0.9997	4352

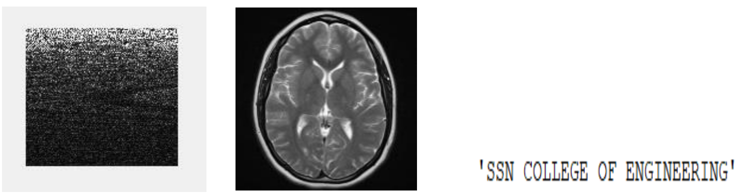
The original image, stego image and the encrypted data is shown in the Figure 11.



(a) (b) (c)

Figure 11. (a) Original image b) Stego image
c) Encrypted data

The stego image is subjected to encryption and the encrypted ciphertext is decrypted and de-embedded to get back the original image. The encrypted cipher text, recovered image and the data extracted is shown in Figure 12.



(a) (b) (c)

Figure 12: (a) Ciphertext b) Recovered Image c) Extracted Data

The comparison of embedding capacity for existing method and proposed method is shown in Table 6. The proposed DPM method achieved better embedding capacity than the existing method. The security issues for proposed method and existing method are concerned. The PSNR of recovered cover image under various attacks for Proposed DPM algorithm and existing algorithm is shown in Table 7 and Table 8.

Table. 6 Comparison Of EC For DPM And Proposed Method

Test Image	DPM	Proposed Method
Brain	19535	25755
Heart	6067	9057
CT-Liver	18897	28751
Molecular	1166	1856
Celulas	2514	2968

Table.7 PSNR of recovered cover image under various attacks for proposed DPM algorithm

Attack	Level	Brain	Heart	Liver	Molecular	Celulas
Additive Noise	0.5%	45.3	46.7	45.9	44.1	42.3
JPEG Compression	5:1	44.2	43.6	42.1	42.4	41.7
Rotation	5	44.5	42.3	44.4	42.8	41.9
Median Filter	3x3	43.5	44.1	44.5	41.3	41.5

Table 8. Percentage of covered image under various attacks for DPM algorithm

Attack	Level	Brain	Heart	Liver	Molecular	Celulas
Additive Noise	0.5%	38.7	36.9	41.2	43.6	41.5
JPEG Compression	5:1	37.4	35.8	41.4	41.2	40.6
Rotation	5	38.4	35.1	40.8	40.5	40.0
Median Filter	3x3	37.1	35.3	40.1	40.9	40.1

IV CONCLUSION

This paper describes the method in which the cover image is embedded with encrypted data by using Difference Pair Expansion Method and is subjected to encryption by using Double Image Encryption

Compression technique. Encrypting the image after embedding provides high practical security. On the receiver side the encrypted stego image undergoes the reverse process of embedding and encryption to recover the original image and data. The experimental results showed that our proposed scheme achieved better embedding capacity than the other schemes.

REFERENCES

[1]. He, Wenguang, Zhanchuan Cai (2020) "*High-fidelity Reversible Image Watermarking Based on Effective Prediction Error-Pairs Modification*", IEEE Transactions on Multimedia.Vol.23, No.8, pp. 248-259.

[2]. S.-W. Weng, Y.-Q. Shi, W. Hong, and Y. Yao, (2019) "*Dynamic improved pixel value ordering reversible data hiding,*" Inf. Sci., Vol. 489, No. 7, pp. 136–154.

[3]. W.-G. He, G.-Q. Xiong Cai and Y.-M Wang, (2018) "*Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion,"* Inf. Sci., Vol. 467, No. 5, pp. 784–799.

[4]. W.G. He, J. Cai, K. Zhou, and G.-Q. Xiong, (2017) *"Efficient PVO-based reversible data hiding using multistage blocking and prediction accuracy matrix,"* J. Vis. Commun. Image Representation, Vol. 46, No. 3, pp. 148-161.

[5]. J.Tian, (2003), *"Reversible data embedding using a difference expansion*" IEEE Trans. Circuits Syst. Vol.13, pp. 890–896.

[6]. X. Qu and H. J. Kim, (2015) *"Pixel-based pixel value ordering predictor for high fidelity reversible data hiding,"* Signal Process., Vol. 111, No. 3, pp. 249–260.

[7]. D.M. Thodi, J.J. Rodriguez (2007), *Expansion embedding techniques for reversible watermarking*, IEEE Trans. Image Process.16(3) Vol.16, No. 7, pp. 721–730.

[8]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, (2011) *"Reversible watermarking algorithm using sorting and prediction,"* IEEE Trans. Circuits Syst. Video Technol., Vol. 19, No. 7, pp. 989–999.

[9]. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, (2010) *"Reversible image watermarking using interpolation technique,"* IEEE Trans. Inf. Forensics Secur., Vol. 5, No. 1, pp. 187–193.

[10]. X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, (2009) *"Lossless data embedding using generalized statistical quantity histogram,"* IEEE Trans. Circuits Syst.Video Technol., Vol. 21, No. 8, pp. 1061–1070.

[11]. Changtao He, Zhigang Liu, Xudong Chen, Jun Wang, (2020) *"Double-image asymmetric cryptosystem using cylindrical diffraction and spectrum fusion and compression",* IET Optoelectron., Vol. 14, No. 4, pp. 169-175.

[12]. Chen, W., Chen, X. (2011*) 'Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain'*, Opt. Commun., Vol. 284, No. 16 pp. 3913–3917.

[13]. Chen, J.X., Zhu, Z.L., Fu, C., et al. (2015) *'Analysis and improvement of a double image encryption scheme using pixel scrambling technique in gyrator domains'*, Opt. Laser Eng., Vol. 66, pp. 1–9.

[14].Chen, J., Zhu, Z., Liu, Z., et al. (2014) *'A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains'*, Opt. Express, Vol. 22, pp. 7349–7361.

[15].Kumar, R., Sheridan, J.T., Bhaduri, B. (2018) *'Nonlinear double-image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm'*, Opt. Laser Technol., Vol. 107, pp. 353–360.

[16].Liu, S., Guo, C., Sheridan, J.T. (2014) *'A review of optical image encryption techniques',* Opt. Laser Technol., Vol. 57, pp. 327–342.

[17].Li, L. (2009) *'Image encryption based on gyrator transform and two-step phase shifting interferometry',* Opt. Lasers Eng., Vol. 47, pp. 45–50.

[18].Liu, Z., Xu, L., Lin, C., et al. (2010) *'Image encryption by encoding with a nonuniform optical beam in gyrator transforms domains',* Appl. Opt., Vol. 49, pp. 5632–5637.

[19].Liu, Z.J., Li, Q.M., Dai, J.M., et al. (2009) *'A new kind of double-image encryption by using a cutting spectrum in the 1D fractional Fourier transform domains',* Opt. Commun., Vol. 282, pp. 1536–1540.

[20]. Liu, Z.J., Guo, Q., Xu, L., et al. (2010) *'Double-image encryption by using iterative random binary encoding in gyrator domains',* Opt. Express, Vol. 18, pp.12033–12043.