Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, July 2021:2923- 2937

Research Article

Visual Secret Sharing Scheme using Dual Block scrambling and DWT based Encryption on JPEG Images

Muhammed Kabeer P[1], Ranju S. Kartha[2]

Abstract

Visual Secret sharing structure with the concept of two shares also names as transparencies. The host images generated the first share, then other share is randomly developed by the user, but here the user identity can be revealed very easily. So for improving the security and privacy of the users, k-n sharing secret scheme can be used. It is a kind of visual cryptographic technique, where a minimum assembly of k out of the n shares are required to reveal the secret data. Visual cryptography allows the data (images, text, etc.) can be encrypted in a such way that the data received can be decrypted as a visual image. In this paper, the dual block scrambling-based encryption system is used for improving the security of JPEG images. The proposed methodology uses encryption-then compression (EtC) schemes with DWT (Discrete wavelet transform) compression on JPEG images, enables the use of small block size through an untrusted channel. This technique is very useful in the banking sector where we need high secured banking application like locker system, in this situation multiple users can handle the same transaction. This structure is enhanced to improve the security counter to the various fraud attacks such as puzzle solver and brute-force attacks.

Keywords: *Discrete wavelet transform, Encryption-then compression, k-n secret sharing system, Advanced Encryption Standard.*

Introduction

The security for information is becoming more significant in nowadays, while the broadcasting or storing the data. In several developments the information is embedded in the images. Then, the protection of these images from the unofficial contact is very important. In this field of hiding the information is done by encrypting the images. Hiding the images or image encryption methods and its algorithm series from the spatial simple domain procedure are complicated and dependable domain frequency (Krikor 2009). The rapid increase of mobile network, cloud computing, internet of things, and social networking, the security issues of the transmission of images becomes

[1] PG Student, Mangalam College of Engineering, Ettumanoor, Kerala, Computer Science and Engineering Department, kabeer4it@gmail.com

[2] Associate Professor/ Dr., Mangalam College of Engineering, Ettumanoor, Kerala, Computer Science and Engineering Department, kabeer4it@gmail.com

Received: , Accepted:

crucial. The encryption algorithm for images should meet the requirements of secure transmission and storage of JPEG images in different applications (Abdmouleh 2017).

The visual secret sharing scheme (VSS) is used to shared images that are handwritten notes, pictures or printed text and that is observable by gathering k or more participants with their images by means of a projector overhead (Yang and Laih 2000). In a cryptographic visual scheme, n shares of binary prototype is programmed the binary image secret. By superimposing a set of qualified transparencies it is possible to decrypt the original secret messages visually. This method, which uses a one-way function as data encryption. Without using the secret key, the calculation becomes complex and which requires a huge amount of time so it assures security.

The Discrete Wavelet Transform (DWT) is also termed as compression block, which compresses a set of DWT distinct blocks. This intern can be used as transformation method in data compression and signal processing. The encryption of JPEG images can be enhanced by encrypting DWT coefficients. The DWT coefficient tables are formulated by way of various tests and experiments, which is understandable for all users, so that can be vulnerable to attacks.(Lian, Sun, and Wang, n.d.) The AC coefficients from the image compression process are used for encryption. In this technique the DC coefficient is not used for any computation because they are carrying significant visible data, so the secret image perdition can be easily done (P. Li and Lo 2019).
This paper proposes a new method of block scrambling-based image encryption system for EtC and k-n secret sharing system which helps to enhance the safety associated with the conventional system (Sirichotedumrong et al. 2019). This method uses small block size, so the amount of blocks used is very large, that also enhances the security and invisibility against the attacks and makes the EtC system more robust (Sirichotedumrong, Chuman, and Kiya 2018). The compression performance is very high when the images from EtC schemes were uploaded and downloaded from social media.

The remaining part of this section describes about the work structure as follows; section 2 defines highlight of previous effort that are done by the scholars in this domain with more experimental tasks; Part 3 describes the methodologies used; part 4 comprises the proposed system architecture; and Part 6 involves discussion on results. Part 8 discusses the conclusion and future work.

Literature Review

Anu et. al. proposes a new secret sharing scheme which uses AES algorithm for encryption, and encryption was carried out using a secret key generated from a genetic algorithm. After encryption, the result is divided into k shares according to the input from the n users (Anu, 2020). The original secret image can reconstructed by carrying out the AES decryption on k shares. Here the genetic algorithm uses complex measures to create the secret key so the it enhances the security of the secret sharing scheme.

Tatsuya et al. proposes a block scrambling based encryption to enhance the security against jigsaw puzzle solver attacks. This technique uses the geometric transformation and color transformation during block scrambling

process. Geometric transformation involves block scrambling, block rotation and block inversion (Tatsuya, 2018)In color transformation, positive-negative transformation and color scrambling. The series of these steps makes this algorithm more secure when compared to the traditional methods.

Kenta et. al. proposes a EtC system based on JPEG XR/JPEG-LS encryption mechanism which provides good compression performance when compared to the system which uses same encryption process without compression process (Kenta 2017). Here the sender uses a shared secret key for encryption and this process involves four block based encryption steps. The output of encryption process is applied to JPEG/XR coding for compression. At the receiver side the decomposition will takes place before decryption.

Youxia et. al. proposes a new image encryption scheme based on the discrete wavelet transform (DWT) and Schur decomposition. The encryption process first performs RSA algorithm, the chaotic system generates a sequence of random values which is used for performing diffusion and confusion (Youxia 2021). Then output is applied to Schur decomposition and the DWT transformation is carried out on the cover image and both will embed together. Then IDWT transformation is applied and perform inverse scrambling operations. This encryption process includes large number of steps so it takes lots of time. It can be improved by including compression techniques.

Methodology

This section describes the general structure and proposed methodology based on new novel methods - block scrambling based image encryption method for EtC system to enhance the security and k-n secret sharing systems with JPEG compression, when compare with the conventional scheme.

DWT Compression

The techniques used for the multi-resolution images decomposition by Discrete wavelet Transform (DWT) is shown in Figure 1 (Wang 2009). At the initial stage, an image is disintegrated into the 4 sub-bands they are; HL1, HH1,LH1 and LL1, where the HH1, HL1 and LH1 is represented as the wavelet scale finest coefficient, this is known as detailed image, while the LL1 that stands for the level of course coefficients this is known as approximation images. To attained the next level of course coefficient wavelet, then the LL1 sub-band is more disintegrated into the 4 sub-bands as HL2, HH2, LH2, and LL2. According to the application of user's, this process of decomposition that continues till it reached the certain final scale.

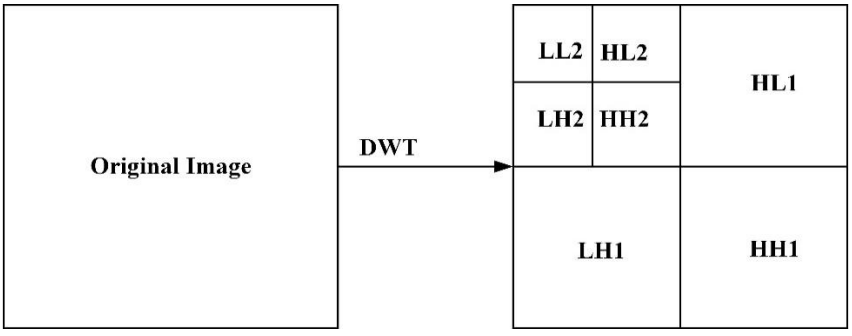


Figure 1. Two-level DWT of an image

The JPEG encoding represents the color images is transformed from the RGB to YCbCr, image disintegrated into 8X8 block, this block is converted from the frequency area to the spatial area by applying DWT compression. Each coefficient DWT compression is separated by the constant equivalent in a quantization table which is then rounded into the adjacent numeral, and the DWT coefficients are skimmed in a predefined order that can be used in last step. The sensitivity of Human visual system (HVS) is less in high frequency, so the significant visual structures of the image are positioned in the low frequency and the sensitive information is placed in high frequency (Han 2013).

Advanced Encryption Standard (AES)

The AES processes a block of 128 bits size as input. It can be support by three various key length of 256, 192 and 128 bits and the number of rounds depends on the size of the key. The first round involves four different transformation parameter: Mix Column, Add Round Key, Shift Rows and Sub bytes. Then the three transformation on final round. Each of the transformation process takes on 4X4 matrices. The decryption involves reverse of all these four rounds.

k-n Secret Sharing Scheme

This proposed system first divides the secret image into n shares according the k-n secret sharing scheme and each shares are subjected to dual block scrambling and DWT based compression that ensures security.

Enhanced Security

This proposed method has a greater features when compared with the conventional encryption method that in terms of the size of blocks and the blocks quantity. Then the encrypted images are produced by the proposed system are grayscale ones.

- Block Size is Small
- Large Blocks Number
- Less color information in Blocks
- Expansion of Key space

Proposed System Architecture

In this model, initially at the encryption process the secret image is divided into n shares using k-n secret sharing scheme and each shares are encrypted separately. After AES encryption, the encryption and decryption of the image process is performed by DWT Compression and Inverse DWT (IDWT) compression technique. Thus, the blocks are converted from the spatial area to the frequency area using the coefficient of DWT. After DWT

compression, the encrypted images are divided into n shares. These encrypted images are decrypted by using the IDWT compression techniques. After IDWT transformation the original image can be retrieved by using the human visual system (HVS).

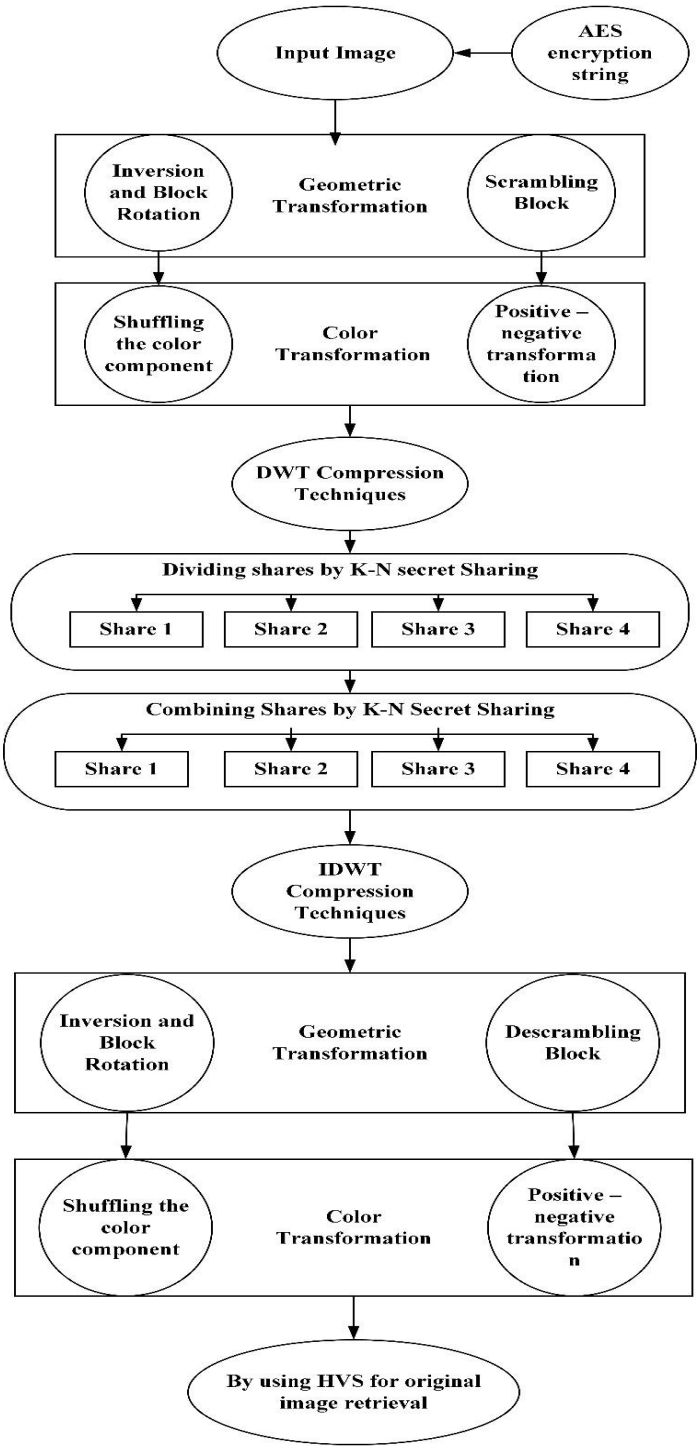


Figure 2. Proposed System Architecture

Block Scrambling-Based Image Encryption

The proposed system uses, the block-scrambling based Image encryption system so it provides system security against the puzzle solver and brute-force attackers.

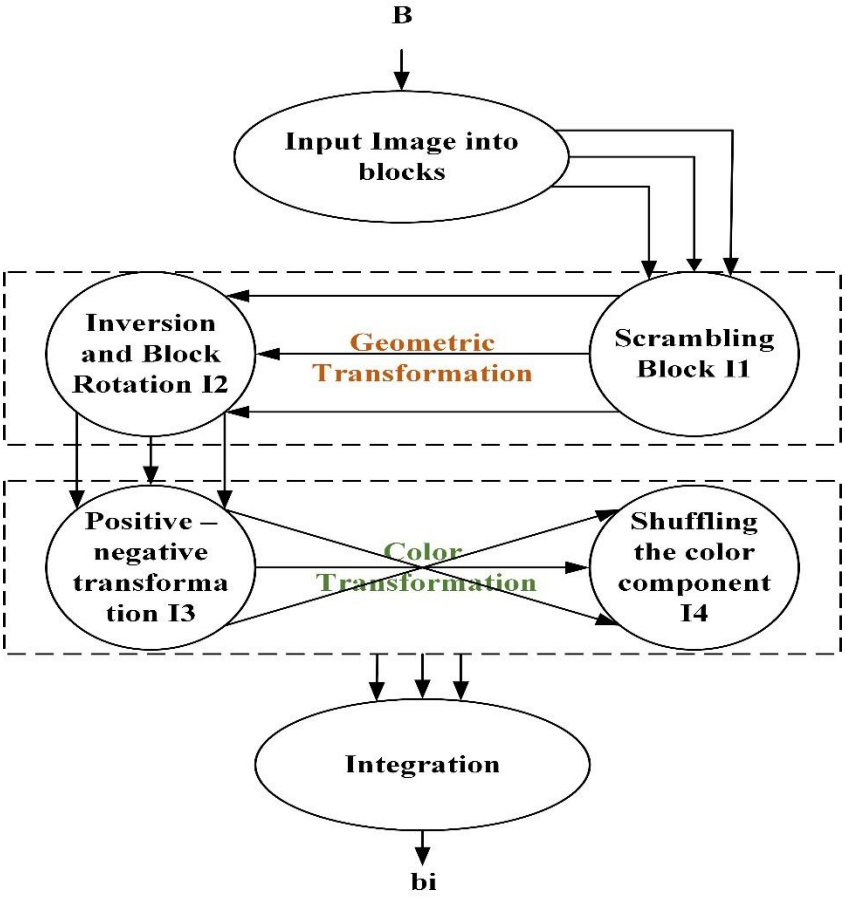


Figure 3. Process of Scrambling encryption method

An image with a pixel of X ×Y is initially divided into a non-overlapped block includes $O_x \times O_y$ pixels; the block scrambling-based process includes four stages that are useful for separating the image. Figure 3. shows the technique with $O_x = O_y = 16$, in this research, $O_x = O_y = 16$ is used for performing the method of image encoding to produce an encrypted image $b_{i,}$ which includes the following step:

1. The X × Y pixels image is divided into blocks, each blocks having $O_x \times O_y$ pixels, and the divided blocks are permuted randomly using an integer which is generated from the random secret key $I_{1.}$

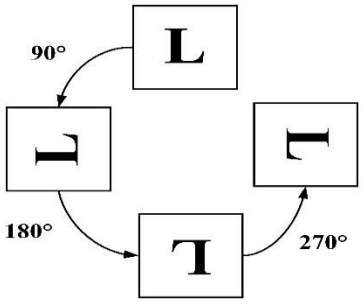


Figure 4. Block Rotation

2. Block inversion and block rotation in shown in Figure 4, that depends on the random number generated the key $I_{2,}$ which is common for all the color components.

3. Negative-positive transformation is applied on individual block that using a binary random integer that are produced by a key I_3, where I_3 is also common to all the color components. In this stage, a value of pixel transformed in the i^{th} block as O_i, V′ is calculated using

$$V' = \begin{cases} v, & (n(j) = 0 \\ v \oplus (2^L - 1), & (n(j) = 1' \end{cases}$$

Where n(j) is a binary arbitrary number produced by I_3, and v ϵ O_i is the rate of pixel on the unique image with L per bit pixel, the occurrence rate probability v(n(j))= 0.5 is used to convert the randomly moments.

4. The three components of color get shuffled individually by a random integer using key I_4.

The image encryption is used in EtC schemes has a block size is limited to $O_x = O_y = 16$, so the effect of color sub-sampling can be avoided. In the standard JPEG, by applying the color sub-sampling to the components chroma as C_r and C_b is encoded in color image, the chroma sub-sampled mechanisms are incorporated to reproduce the identical determination of the original image.

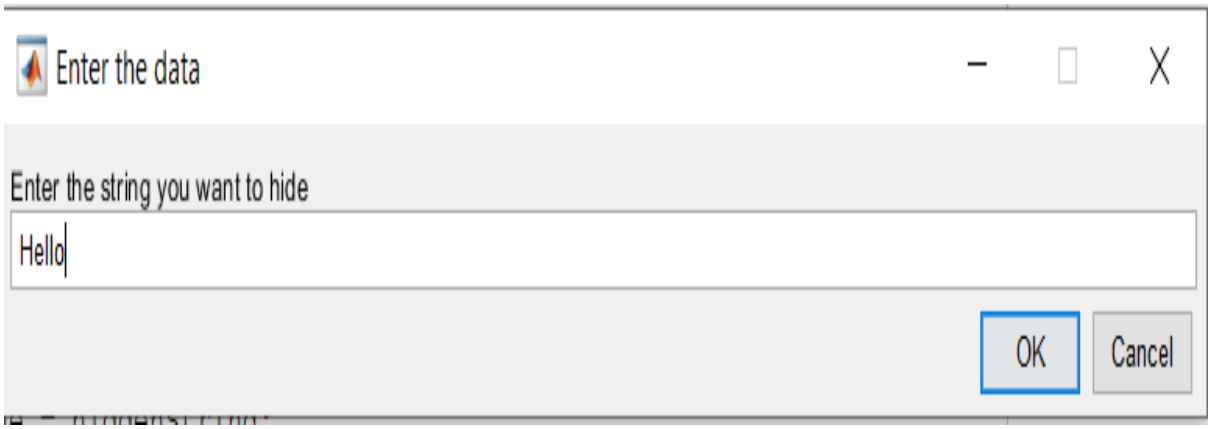
Image Encryption

The image encryption performs the DWT based encryption on each blocks and initially it finds the DWT coefficients and encryption is performed using the coefficients and the randomly generated secret keys.

Result and discussion

The proposed system has been built to enhance the image security by the process of encryption and decryption method. Figure 5. shows the data enter for the process to begin.

Figure 5. Input to the proposed system



```
hiddenString =

    '0024QQz3JojsZF9HJTi/flUREQ=='
```

Figure 6. AES hidden string

Figure 6. shows the performance of AES algorithm that the input images that allows the 128, 192, 256-bit encryption. This symmetrical encryption is more feasible, when compared with asymmetrical encryption that are used in database system.

Figure 7. Input Image, Scrambled Image, Rotated Image, Color Transformation

Figure 7. shows the input images for the compression techniques, then it enters into the process of geometric transformation that includes the methods of block scrambling method, block rotation and block inversion method. The images are got scrambled, then the scrambled image shown in Figure 7. After block rotation the image is as shown in Figure 7. then the data enters into the color transformation process after color transformation image is as shown as Figure 7.

After the color transformation of the shuffled image which is applied into the Discrete Wavelet Transform (DWT) for the process of the encryption, then after the process of encryption, the images are divided into the amount of shares by using the K-N secret sharing method.

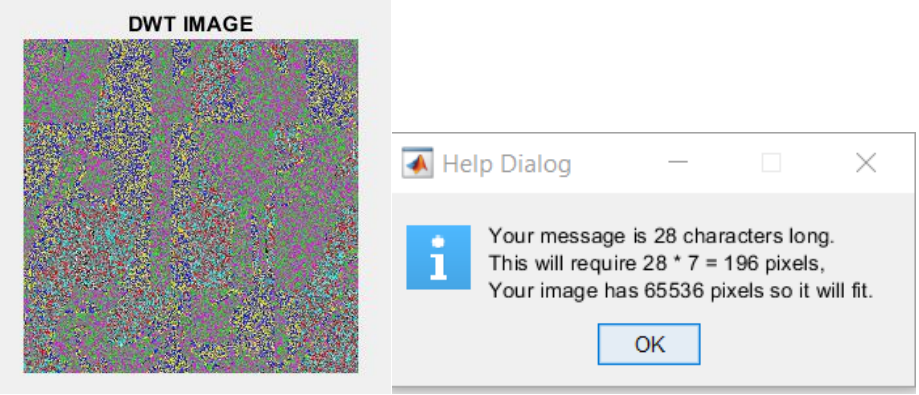


Figure 8. DWT image and encrypted bits

Figure. 8 shows the image after the encryption process, Then it is divided into n shares. In the decryption process, the decryption can be done by using the descrambling method. Figure 9. shows the original gray scale cover image and the hidden string of our image by AES method, to retrieve the original image.

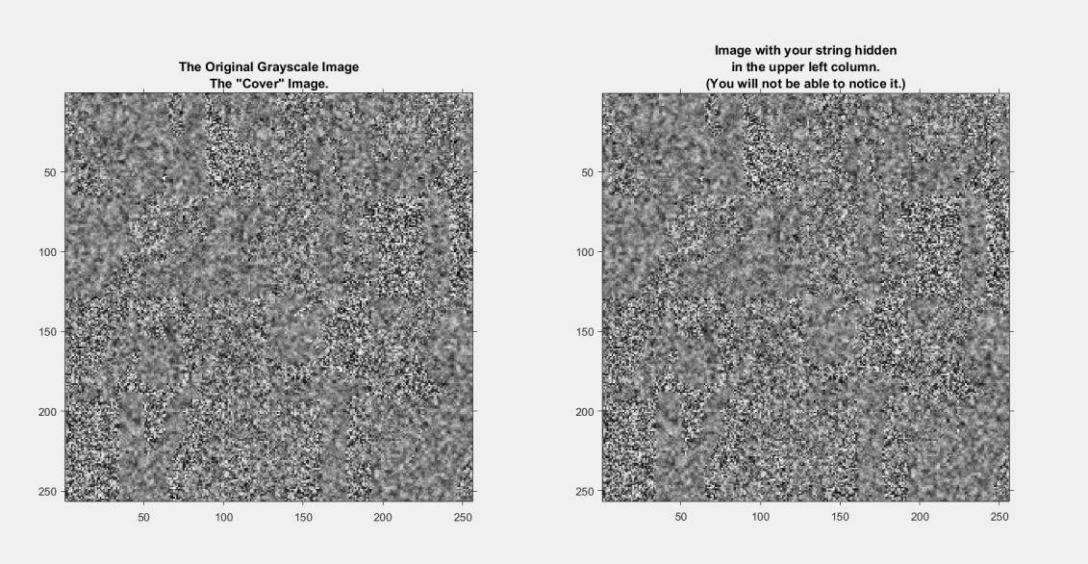


Figure 9. The original gray scale cover image and the hidden string

Figure 9. shows the hidden string which is got recovered “Hello” by using the original gray-scale to the cover images. Then combining the divided shares by using the K-N secret sharing method. The merging of k shares is shown in Figure 10.

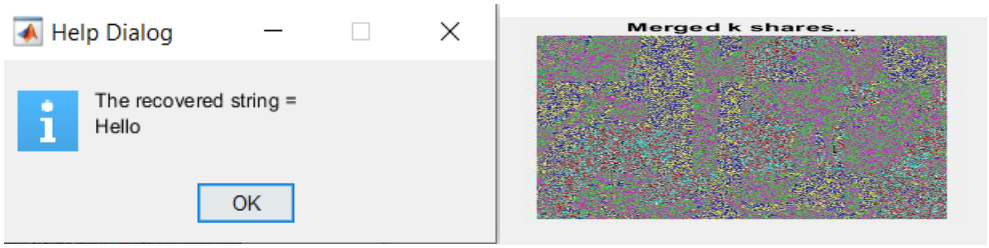


Figure 10. Merging k shares

Then finally the decryption process is done by using the inverse DWT method. Then each of the image share get decoded as shown on the Figure.11.

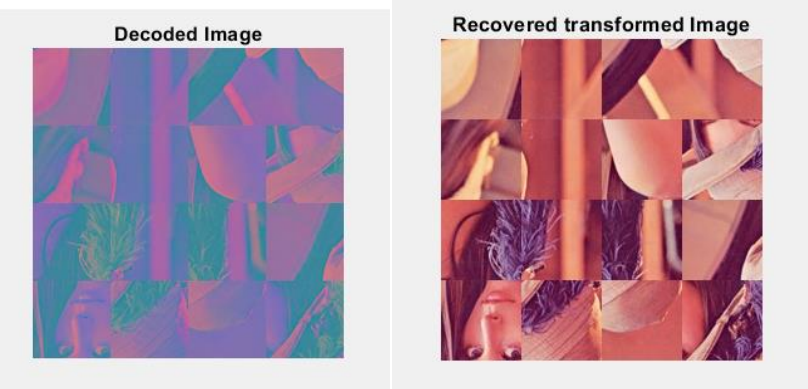


Figure 11. Decoded Image, Recovered Transformed Image

After the decryption process, the images are get recovered into the transformed recovered image and then the each of the shared image are get descrambled on the decryption process. The descrambled into original image is shown in Figure 12.

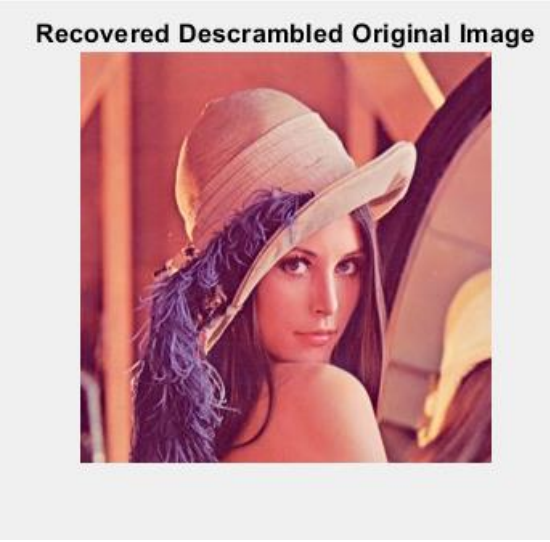


Figure 12. Descrambled Image

The proposed method enhances the security of images by hidding the data by using the K-N secret sharing method used for the image verification. Applying the encryption and decryption process by DWT and IDWT compression method on various images, the experimental results from this process are given below:

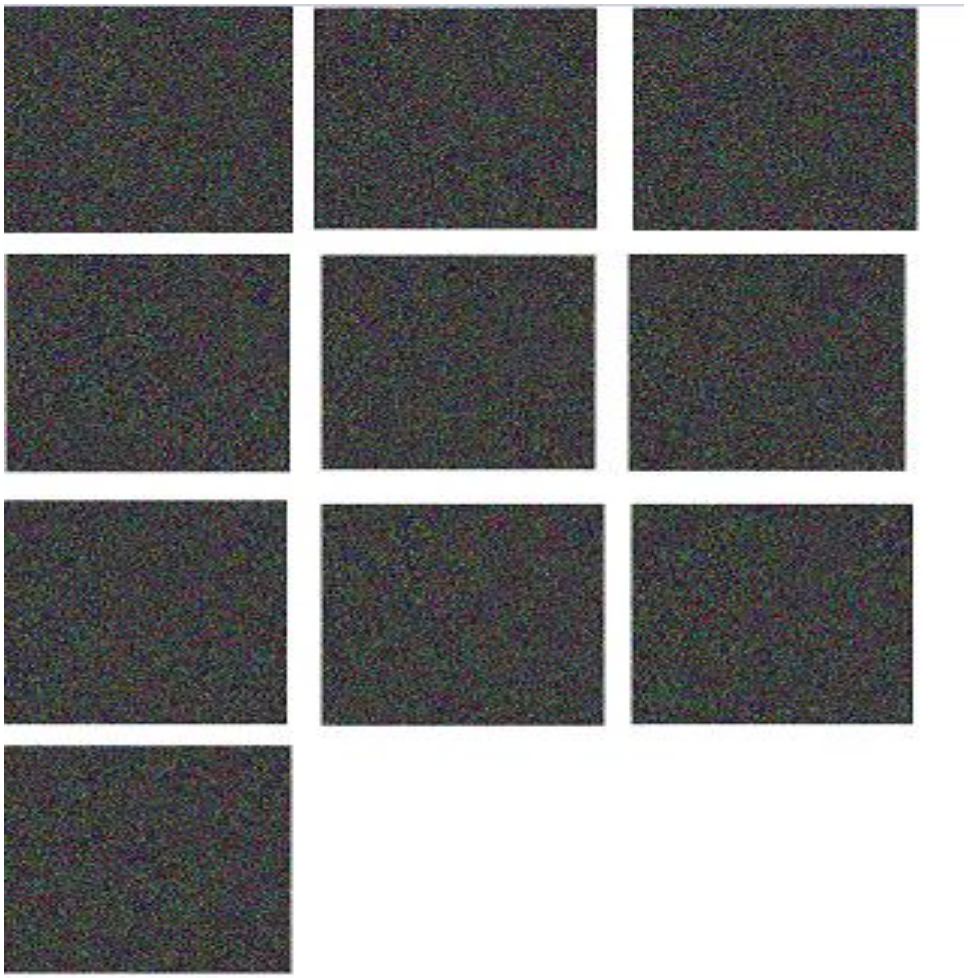


Figure 13. Ten shared image that look like noise obtained from the proposed System

Figure 13. shows the ten number of shares that shared among n users using the k-n secret sharing algorithm. There are ten number of images that are obtained by dividing the scrambled blocks and shared among n users, the output looks in the form of noise images. Each of the shared image has a secret data. Here, this encryption system improves the security of EtC system with the JPEG compression. These features improves the security of the secret images against the various attacks.

Table 1. Comparison among Various Image Encryption Techniques

Sl.No	Author	Method	PSNR (in dB)	Mean Square Error (MSE)
1	(Masood et al. 2020) / 2020	3D Lorenz Chaotic Maps; Hybrid Dynamical system	7.9dB	error
2	(Khan and Masood 2019)/ 2019	Multiple chaotic maps	7.76 dB	0.1
3	(Yao et al. 2020)/ 2020	Discrete Trinion Fourier Transform, multiresolution singular value decomposition	13.54dB	0.0011
4	(T. Wang and Wang 2020)/ 2020	Bit-level permutation, Hyper-chaos	8.66dB	0.09
5	Proposed Method/ 2021	DWT encryption method	26.99dB	0.5372

Conclusion

This paper proposes a new k-n secret sharing scheme by combining two techniques: block scrambling on image encryption system and EtC scheme for JPEG images. On the time of dividing a secret image into several number of n shares, secret keys are generated randomly. The proposed algorithm uses a block size $B_x = B_y = 16$, by reducing the block size $B_x = B_y = 8$, the security of the secret image can be improved against the robustness of cipher text attacks. This technique requires very low mathematical computations when compare with another existing method of the color image visual cryptography. This method only forms '1' at the position bit and that separate the '1' into the (n-k+1) shares using the random integer. From the result, individual share that does not reflects a very small or even no data regarding to the original image to the human eye. So it is concluded that the proposed method system has a good performance than the conventional color image visual cryptography.

References

1. Anu G S , Geethos Ninan,(2020), K-N Secret Sharing Scheme Encrypting Multiple Images in Visual Cryptography, International Journal of Science and Research (IJSR,Volume 9 Issue 7.
2. Kenta KURIHARA, Shoko IMAIZUMI, Sayaka SHIOTA, Hitoshi KIYA, (2017), An Encryption-then-Compression System for Lossless Image Compression Standards, IEICE Transactions on Information and Systems, Volume E100.D (2017) Issue 1.
3. Youxia Dong, Xiaoling Huang, and Guodong Ye, (2021), Visually Meaningful Image Encryption Scheme Based on DWT and Schur Decomposition, Security and Communication Networks, Volume 1, Article ID 6677325: https://doi.org/10.1155/2021/6677325.

4. Tatsuya Chuman, Kenta Kurihara, Hitoshi Kiya, (2018), On the Security of Block Scrambling-Based EtC Systems against Extended Jigsaw Puzzle Solver Attacks, IEICE Transactions on Information and Systems E101.D(1):37-44.
5. Abdmouleh, Med Karim, Ali Khalfallah, and Med Salim Bouhlel. 2017. "A Novel Selective Encryption Scheme for Medical Images Transmission Based-on JPEG Compression Algorithm." Procedia Computer Science 112: 369–76. https://doi.org/10.1016/j.procs.2017.08.026.
6. Arunkumar, M, and S Prabu. 2014. "Implementation of Encrypted Image Compression Using Resolution Progressive Compression Scheme." International Journal of Computer Science and Mobile Computing (IJCSMC) 3 (6): 585590.
7. Chang, Xiangyu, Aimin Yan, and Hongbo Zhang. 2020. "Ciphertext-Only Attack on Optical Scanning Cryptography." Optics and Lasers in Engineering 126: 105901.
8. Chuman, Tatsuya, Warit Sirichotedumrong, and Hitoshi Kiya. 2018. "Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for Jpeg Images." IEEE Transactions on Information Forensics and Security 14 (6): 1515–25.
9. Droste, Stefan, and N Koblitz. n.d. "New Results on Visual Cryptography," 15.
10. Furht, Borko. 1995. "A Survey of Multimedia Compression Techniques and Standards. Part I: JPEG Standard." Real-Time Imaging 1 (1): 49–67.
11. Han, Yanyan, Yixiao Shang, and Wencai He. 2013. "DWT-Domain Dual Watermarking Algorithm of Color Image Based on Visual Cryptography." In 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 373–78. IEEE.
12. Iida, Kenta, and Hitoshi Kiya. 2019. "Image Identification of Grayscale-Based JPEG Images for Privacy-Preserving Photo Sharing Services." In 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 1750–55. IEEE.
13. Jalaleddine, Sateh MS, Chriswell G Hutchens, Robert D Strattan, and William A Coberly. 1990. "ECG Data Compression Techniques-a Unified Approach." IEEE Transactions on Biomedical Engineering 37 (4): 329–43.
14. Kalubandi, Venkata Krishna Pavan, Hemanth Vaddi, Vishnu Ramineni, and Agilandeeswari Loganathan. 2016. "School of Information Technology, VIT Vellore.," 6.
15. Kandar, Shyamalendu, and Bibhas Chandra Dhara. 2011. "Kn Secret Sharing Visual Cryptography Scheme on Color Image Using Random Sequence." International Journal of Computer Applications 25 (11): 0975–8887.
16. Kandar, Shyamalendu, Arnab Maiti, and Bibhas Chandra Dhara. 2011. "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking." International Journal of Computer Science Issues (IJCSI) 8 (3): 543.
17. Khan, Majid, and Fawad Masood. 2019. "A Novel Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps." Multimedia Tools and Applications 78 (18): 26203–22.
18. Krikor, Lala, Sami Baba, Thawar Arif, and Zyad Shaaban. n.d. "Image Encryption Using DCT and Stream Cipher," 12.

19. Lay, Jose A, and Ling Guan. 1999. “Image Retrieval Based on Energy Histograms of the Low Frequency DCT Coefficients.” In 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No. 99CH36258), 6:3009–12. IEEE.
20. Li, Chengqing, Dongdong Lin, and Jinhu Lü. 2017. “Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits.” IEEE MultiMedia 24 (3): 64–71.
21. Li, Peiya, and Kwok-Tung Lo. 2019. “Joint Image Encryption and Compression Schemes Based on 16$\times$ 16 DCT.” Journal of Visual Communication and Image Representation 58: 12–24.
22. Li, Shujun, Chengqing Li, Guanrong Chen, Dan Zhang, and Nikolaos G Bourbakis. 2004. “A General Cryptanalysis of Permutation-Only Multimedia Encryption Algorithms.” IACR’s Cryptology EPrint Archive: Report 374: 2004.
23. Lian, Shiguo, Jinsheng Sun, and Zhiquan Wang. n.d. “A Novel Image Encryption Scheme Based-on JPEG Encoding,” 4.
24. Lin, Shinfeng D., Shih-Chieh Shie, and J.Y. Guo. 2010. “Improving the Robustness of DCT-Based Image Watermarking against JPEG Compression.” Computer Standards & Interfaces 32 (1–2): 54–60. https://doi.org/10.1016/j.csi.2009.06.004.
25. Liu, Ting Yu, Kuan Jen Lin, and Hsi Chun Wu. 2017. “ECG Data Encryption Then Compression Using Singular Value Decomposition.” IEEE Journal of Biomedical and Health Informatics 22 (3): 707–13.
26. Liu, Wei, Wenjun Zeng, Lina Dong, and Qiuming Yao. 2009. “Efficient Compression of Encrypted Grayscale Images.” IEEE Transactions on Image Processing 19 (4): 1097–1102.
27. Liu, Yanlin, Jingbing Li, Jing Liu, Uzair Aslam Bhatti, Yanwei Chen, and Shihui Hu. 2019. “Watermarking Algorithm for Encrypted Medical Image Based on DCT-DFRFT.” In Innovation in Medicine and Healthcare Systems, and Multimedia, 105–14. Springer.
28. Masood, Fawad, Jawad Ahmad, Syed Aziz Shah, Sajjad Shaukat Jamal, and Iqtadar Hussain. 2020. “A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map,” 28.
29. Patel, Komal D, and Sonal Belani. 2011. “Image Encryption Using Different Techniques: A Review.” International Journal of Emerging Technology and Advanced Engineering 1 (1): 30–34.
30. Petrushan, M, Yu Vermenko, D Shaposhnikov, and S Anishchenko. 2013. “Comparative Analysis of Color-and Grayscale-Based Feature Descriptions for Image Recognition.” Pattern Recognition and Image Analysis 23 (3): 415–18.
31. Radharani, S, and ML Valarmathi. 2011. “Multiple Watermarking Scheme for Image Authentication and Copyright Protection Using Wavelet Based Texture Properties and Visual Cryptography.” International Journal of Computer Applications 23 (3): 29–36.
32. Shankar, K, and P Eswaran. 2017. “RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography.” China Communications, 13.
33. Sirichotedumrong, Warit, Tatsuya Chuman, and Hitoshi Kiya. 2018. “Compression Performance of Grayscale-Based Image Encryption for Encryption-Then-Compression Systems.” ArXiv Preprint ArXiv:1810.13067.

34. Sirichotedumrong, Warit, and Hitoshi Kiya. 2019. “Grayscale-Based Block Scrambling Image Encryption Using Ycbcr Color Space for Encryption-Then-Compression Systems.” APSIPA Transactions on Signal and Information Processing 8.
35. Sirichotedumrong, Warit, Takahiro Maekawa, Yuma Kinoshita, and Hitoshi Kiya. 2019. “Privacy-Preserving Deep Neural Networks with Pixel-Based Image Encryption Considering Data Augmentation in the Encrypted Domain.” In 2019 IEEE International Conference on Image Processing (ICIP), 674–78. IEEE.
36. Tuncer, Türker, and Engin Avci. 2016. “A Reversible Data Hiding Algorithm Based on Probabilistic DNA-XOR Secret Sharing Scheme for Color Images,” 8.
37. Wang, Ming-Shi, and Wei-Che Chen. 2009. “A Hybrid DWT-SVD Copyright Protection Scheme Based on k-Means Clustering and Visual Cryptography.” Computer Standards & Interfaces 31 (4): 757–62. https://doi.org/10.1016/j.csi.2008.09.003.
38. Wang, Tao, and Ming-hui Wang. 2020. “Hyperchaotic Image Encryption Algorithm Based on Bit-Level Permutation and DNA Encoding.” Optics & Laser Technology 132: 106355.
39. Wu, Xiangjun, Haibin Kan, and Jürgen Kurths. 2015. “A New Color Image Encryption Scheme Based on DNA Sequences and Multiple Improved 1D Chaotic Maps.” Applied Soft Computing 37: 24–39.
40. Yang, Ching-Nung, and Chi-Sung Laih. 2000. “New Colored Visual Secret Sharing Schemes.” Designs, Codes and Cryptography 20 (3): 325–36.
41. Yao, Qijun, Zhuhong Shao, Yuanyuan Shang, Hui Ding, Xilin Liu, Rui Zeng, and Qingbin Tong. 2020. “Color Image Encryption Based on Discrete Trinion Fourier Transform and Random-Multiresolution Singular Value Decomposition.” Multimedia Tools and Applications 79 (37): 27555–81.
42. Ye, Guodong. 2010. “Image Scrambling Encryption Algorithm of Pixel Bit Based on Chaos Map.” Pattern Recognition Letters 31 (5): 347–54.
43. Zhang, Dinghui, and Fengdeng Zhang. 2014. “Chaotic Encryption and Decryption of JPEG Image.” Optik 125 (2): 717–20. https://doi.org/10.1016/j.ijleo.2013.07.069.