Unified Fractional Chaotic Map-imposed Progressive Block-based Visual Cryptography Technique

[1]I.Edwin Dayanand, [2]Dr.R.K.Selva Kumar, [3]Dr.N.R.Ram Mohan
[1]Research scholar,Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India.
[2]Professor, Computer Science and Engineering, CVR College of Engineering, Hyderabad, India.
[3]Assistent Professor, Computer Science and Engineering, Amrita College of Engineering and Technology Nagercoil, Tamilnadu, India.

Abstract-The core objective of secret sharing concentrates on the development of a novel technique that prevents the destroy and leakage of original data during the distribution and encoding processes. Progressive visual cryptography is considered for the potential over the traditional visual cryptography schemes, since the former does not require does not suffer from the limitations of requiring a minimum number of participants during the process of encryption and sharing. The chaotic map-based Progressive visual cryptography is determined to be superior in facilitating predominant secrecy under sharing and encryption. In this paper, a Unified Fractional Chaotic Map-imposed Progressive Block-based Visual Cryptography (UFCM-PBVC) Technique is proposed for enhancing the degree of preventing the leakage and destruction of sensitive information during an exchange and encryption. This proposed UFCM-PBVC technique uses the merits of Henon and Lorentz maps for effective encryption, since it introduces the option of deriving non-linear behavior that results in sequence generation that covers the complete range with proper distribution in order to minimize the degree of leaks in sharing. The simulation results of the proposed UFCM-PBVC technique investigated using entropy, PSNR and Mean Square Error was determined to be improved at an average rate of 27%, 23% and 31% predominant to the baseline visual cryptography approaches considered in the comparison.

Keywords: Progressive visual cryptography, Unified Fractional Chaotic Map, Henon Maps, Lorentz maps, secret sharing.

1. Introduction

In general, the core objective of any secret sharing approach focuses on the process of protecting the leakage and destruction of the original information under the process of sharing and encoding [1]. This issue of protecting the original information has been investigated in a diversified number of classical visual cryptography-inspired schemes [2]. The visual cryptography-based schemes propounded in the literature over the recent years are classified into classical visual cryptography and progressive visual cryptography [3]. In particular, the progressive visual cryptography has been widely explored by most of the researchers for overcoming the limitations of the classical encoding approaches [4]. However, Hou et al. [5] proved that even the method of prone to the recovery of the original information independent to the reduced numbers of participants essential necessitated in the previous approaches. In this context, it is realized that when the shares are random the possibility of protecting the shares from the attacker's eyes are highly meaningful [6]. Thus, chaotic maps are considered to be the better solution for investigating the security of the shared information with a secret key under the progressive visual cryptography considered as random in nature [7]. Further, the application of periodic force can be converted into a non-linear system by the generation of chaotic response sequences [8]. In spite of chaotic oscillation-based computational frameworks contributed to the implementation of reactive visual cryptography schemes over the recent years, the impactful experimental deployment of a chaotic sequence-based progressive visual cryptography scheme that resolves the issue that emerges due to the problem of information leakage still remains an open discussion [9-10].

In this paper, a Unified Fractional Chaotic Map-imposed Progressive Block-based Visual Cryptography (UFCM-PBVC) Technique has contributed to the view to improve the degree, preventing the leakage and destruction of sensitive information during the process information exchange and encryption. This proposed UFCM-PBVC technique is proposed by using the merits of Henon and Lorentz maps for effective encryption by deriving non-linear behavior that results in sequence generation that covers the complete range with proper distribution in order to minimize the degree of leaks in sharing. The simulation experiments of the proposed UFCM-PBVC technique are conducted using the evaluation metrics of entropy, PSNR and Mean Square in order to quantify its predominance over the baseline visual cryptography approaches considered for comparison.

The subsequent sections of the paper are structured as follows. Section 2 presents the literature review of the potential research works that are contributed in the area of visual secret sharing. Section 3 presents the detailed view of the proposed Unified Fractional Chaotic Map-imposed Progressive Block-based Visual Cryptography (UFCM-PBVC) Technique with its role in effective prevention of information leakage under image sharing. Section 4 highlights the results and discussions of the proposed UFCM-PBVC with the benchmarked schemes of the literature. Section 5 concludes the paper with major contributions and scope of the future research.

2. Related Work

Initially, a Visual Secret Sharing (VSSS) scheme using Random grid and void-cluster oriented post processing was proposed for handling the issues of visual quality and pixel expansion during the process of revealing secret image [11]. This VSS scheme enhanced the image quality during the process of reconstruction. Random grid and void-cluster oriented post processing-based VSS scheme was proved to ensure competitive visual quality by contextually eliminating the issue of visual quality and pixel expansion during the process of decryption. Then, a visual cryptographic approach using a (k,n) approach was proposed for

encoding 'k' secret key into 'n' share images [12]. This (k,n)-based visual cryptographic approach also confirmed predominant visual quality by stacking a number of shares that are greater than 'k' in a specific context. A reliable watermarking approach using visual cryptography is contributed for multiple number of cover images [13]. This reliable scheme of watermarking hides the watermark without changing the original characteristics of the cover images. This watermarking scheme initially extracts the feature shares through the application of singular value decomposition, discrete wavelet transforms and scale invariant feature transform. The comprehensive set of features extracted in the initial step is integrated together with the watermark and private key for the construction of secret share. In this mechanism, the secret share need to be registered with the trust authority. In the problem of cover image dispute, the watermark is extracted through the utilization of the private key, secret key and feature shares. This watermarking scheme was confirmed to be robust under diversified attacks that are specific to scaling and rotation.

Further, a novel threshold Random Grid-based VSS scheme was proposed for enhancing the visual quality of the images [14]. This threshold Random Grid-based VSS scheme (RGVSS) is as potent to the (k,n) threshold-based visual cryptographic scheme. This VSS scheme is capable of preventing the issue of pixel expansion since it does not necessitate the design of codebook through the inclusion of random grids. Then, a realizable progressive visual cryptography scheme was proposed using (2,2) block as the primitive element of share images [15]. This realizable progressive visual cryptography scheme facilitated secret encryption and block pair design for e purpose of secret hiding. This realizable progressive visual cryptography scheme is potent in decrypting partial secret and confirming the stacking shares. This realizable progressive visual cryptography scheme demonstrates superior application in the process of share stacking inference, self decryption watermark that is considered as the vital entities of this scheme in a optimal way. A novel candidate block replacement-based preprocessing approach using basis matrix construction was contributed to prevent a number of unessential encryption conditions that are included in the predefined codebook [16]. This candidate block replacement-based preprocessing approach is superior in the process of encoding and decoding the secret image by imposing the restrictions over the number of participants. This approach confirmed that the probability of reconstruction involved in the black pixels and white pixels of the secret image as 1 and 0.5 respectively. This approach confirmed that the contrast value of the input image used for encoding is nearly 50% inseparable to the reconstructed image with any additional computation involved in the cryptographic approach.

Further, another progressive visual cryptography scheme was contributed to gain a clear reconstructed secret image with maximum number of shares [17]. This progressive visual cryptography scheme is a generalized (k,n)-threshold-based image reconstruction approach that does not include any pixel expansion, since it facilitates control access and loss-tolerance for adapting its suitability in over a wide number of applications. This generalized (k,n)-threshold-based image reconstruction approach automatically included the (2,n) threshold-based image reconstruction approach implicitly for providing maximum visual quality. A Region Incrementing Visual Cryptography Scheme (RIVCS) was propounded with a single secret image, which is partitioned into multiple number of secret regions [18]. The first secret region is determined by superimposing at least 2 secret shares, which played in revealing the complete input image through the process of stacking more and more number of shares in the application. This region incrementing visual cryptography scheme eliminates the issue of pixel expansion, color reversal and low contrast. This region incrementing visual cryptography scheme is also enhanced by incorporating the features of extended visual cryptography and traditional region incrementing visual cryptography scheme together. This region incrementing visual cryptography scheme confirmed meaningful number of share images, enhanced security, no color reversal with enhanced contrast and no pixel expansion.

3. The proposed Unified Fractional Chaotic Map-imposed Progressive Block-based Visual Cryptography (UFCM-PBVC) Technique

This proposed Unified Fractional Chaotic Map-imposed Progressive Block-based Visual Cryptography (UFCM-PBVC) Technique facilitates the process of encoding the secret image through a chaotic map generated through a unified map [19]. This unified map is responsible for partitioning the secrets into blocks, such that the benefit of imperceptibility is included in the encoding process. This unified map also improves the strength of the encoding process such that leakage of information is maximum avoided in the encoding process [20]. This unified map is an enhanced form of a chaotic map proposed by Sprott and Zeraoulia that depends on a novel piecewise property definition based on Equation (1)

$$a(k+1) = 1 - 1.4 g_{\alpha}(a(k)) + b(k) \quad (1)$$

$$b(k+1) = 0.3a(k) \quad (2)$$

In this context, α is considered the parameter of bifurcation that ranges between 0 and 1 with the function g_{α} defined in Equation (3)

$$g_{\alpha}(a(k)) = \alpha|a(n)| + (1-\alpha)a^2(k) \quad (3)$$

This utilization of the unified map in visual cryptography scheme has a potential as it can yield a Henon chaotic map depending the value of α converging to zero as defined in Equation (4) and (5)

$$a(k+1) = 1 - 1.4a^2(k) + b(k) \quad (4)$$

$$b(k+1) = 0.3a(k) \quad (5)$$

On the other hand, depending on the value of α assigned to 1 it can yield a Lorentz map as defined in Equation (6) and (7)

$$a(k+1) = 1 - 1.4|a(k)| + b(k) \quad (6)$$

$$b(k+1) = 0.3a(k) \quad (7)$$

Thus, the unified discrete fractional calculus is utilized for defined the fractional unified map using Equation (8) and (9) respectively.

$${}^{c}\Delta_{x}^{y} a(t) = 1 - 1.4 g_{\alpha}(a(t-1+y) + b(t-1+y) - a(t-1+y) \quad (8)$$

$${}^{c}\Delta_{x}^{y} b(t) = 0.3a(t-1+y) + b(t-1+y) \quad (9)$$

This unified fractional unified map is applied over all the pixels that pertains to each block of the input image used for robust progressive visual cryptography. Further, the pixel value checks for 0 and 1. If the value of the pixel is 0, then the pixel value is assigned to $S_{H(k)}(i,j) = C^{0}(a,k)$, Else the value of the pixel is set to $S_{H(k)}(i,j) = C^{1}(a,k)$. In this context, $S_{H(k)}(i,j) = C^{0}(a,k)$ is used for sharing only the white pixels to al the shares and posses al 0's in the first row and second row contains all values as 1's.

In addition, the sharing of black pixels is enforced based on the complete m+1 matrix as defined by Equation (10) and (11)

$$C^{0}(a,k) = [kab] = 0 \text{ if } a = 1; 1 \le b \le m \quad (10)$$

$$C^{1}(a,k) = [kab] = 1 \text{ if } a = 2; 1 \le b \le m \quad (11)$$

Hence, the image block corresponding the shares over the block is constructed by selecting a particular row from the sharing matrix $S_{H(k)}(i,j) = C^{0}(a,k)$ based on the color of the pixel. This process of the visual crypto system is imposed over the entire image based on the sharing matrix defined over $S_{H(k)}(i,j) = C^{m}(a,k)$ blocks.

The pseudo code of the proposed UFCM-PBVC) Technique is presented as follows.

Input: A halftone secret image P that consists of $k * j$ rows and columns.

Output: m number of shares under n=1,2,,,,,,m

Process

1. Generate a m+1 number of share matrices for the purpose of encoding the secret message that possesses the size of 2*n.
2. For each and every pixel under the blocks, the contextual integration of Henon map and Lorentz map are enforced in an optimal manner.
3. Generate a value through the application of unified map based on the characteristics of chaotic maps.
4. Determine and apply the function over the value of x based on the unified map
5. Iterative the process of applying the unified chaotic map for all the pixels of the input image with the pixel $P(a,b) \in B_{IN}(IM)$ for complete set of blocks.
6. If the value of the pixel $P(a,b) \in B_{IN}(IM) = 0$, it corresponds to white pixel with the pixel value set to $S_{H(k)}(i,j) = C^{0}(a,k)$.
7. Else, the value of the pixel $P(a,b) \in B_{IN}(IM) = 1$, it corresponds to black pixel with the pixel value set to $S_{H(k)}(i,j) = C^{1}(a,k)$.

4. Results and discussions

The predominance of the proposed UFCM-PBVC scheme is investigated using Entropy, Mean Square Error, PSNR value and

Table 1 presents the entropy value associated with each share generated by the proposed UFCM-PBVC scheme as well as the benchmarked RIVCS and RTVSS approaches. The proposed UFCM-PBVC scheme is determined to ensure superior entropy value over the benchmarked RIVCS and RTVSS approaches, since the incorporation of unified map increases the prevention of information leakage under the process of encoding. Thus, the entropy value of the proposed UFCM-PBVC scheme is determined to ensure a entropy value, which is 21.42% and 25.32% predominant over the benchmarked RIVCS and RTVSS approaches

Table 1: Entropy value of the proposed UFCM-PBVC under different shares

The progressive schemes used for comparison	Entropy under different number of shares					
	1	2	3	4	5	6
Proposed UFCM-PBVC	0.9812	0.9803	0.9782	0.9775	0.9678	0.9663
RIVCS	0.7821	0.7802	0.7764	0.7761	0.7754	0.7746
RTVSS	0.7512	0.7510	0.7506	0.7503	0.7502	0.7501

Table 2 highlights the Mean Square Error(MSE) associated with each share generated by the proposed UFCM-PBVC scheme as well as the benchmarked RIVCS and RTVSS approaches. The proposed UFCM-PBVC scheme is determined to ensure lesser MSE value over the benchmarked RIVCS and RTVSS approaches, since the integration of Hennon map and . Thus the MSE value of the proposed UFCM-PBVC scheme is determined to be minimized by 8% and 11% predominant over the benchmarked RIVCS and RTVSS approaches.

Table 2: MSE of the proposed UFCM-PBVC under different shares

The progressive schemes used for comparison	MSE under different number of shares					
	1	2	3	4	5	6
Proposed UFCM-PBVC	0.452	0.458	0.463	0.468	0.473	0.478
RIVCS	0.5121	0.5231	0.5242	0.5249	0.5256	0.5265
RTVSS	0.5321	0.5356	0.5368	0.5373	0.5378	0.5383

Table 3 highlights the PSNR associated with each share generated by the proposed UFCM-PBVC scheme as well as the benchmarked RIVCS and RTVSS approaches. The proposed UFCM-PBVC scheme is determined to ensure lesser PSNR value over the benchmarked RIVCS and RTVSS approaches by preventing a reduced number of shares under cryptosystem. Thus the PSNR value of the proposed UFCM-PBVC scheme is determined to be minimized by 11% and 14% predominant over the benchmarked RIVCS and RTVSS approaches.

Table 3: PSNR of the proposed UFCM-PBVC under different shares

The progressive schemes used for comparison	PSNR under different number of shares					
	1	2	3	4	5	6
Proposed UFCM-PBVC	50.231	50.212	50.187	50.176	50.163	50.154
RIVCS	42.563	42.452	42.343	42.321	42.232	42.121
RTVSS	40.121	40.112	40.013	40.011	40.006	39.673

Table 4 highlights the Intensity of Fabrication (IF) associated with each share generated by the proposed UFCM-PBVC scheme as well as the benchmarked RIVCS and RTVSS approaches. The proposed UFCM-PBVC scheme is determined to ensure lesser IF value over the benchmarked RIVCS and RTVSS approaches as it prevents the degree of fabrication by incorporating effective embedding process. Thus the IF value of the proposed UFCM-PBVC scheme is determined to be minimized by 14% and 191% predominant over the benchmarked RIVCS and RTVSS approaches.

Table 4: Intensity of Fabrication (IF) of proposed UFCM-PBVC under different shares

The progressive schemes used for comparison	Intensity of Fabrication (IF) under different number of shares					
	1	2	3	4	5	6
Proposed UFCM-PBVC	0.7812	0.7823	0.7832	0.7843	0.7856	0.7865
RIVCS	0.6421	0.6434	0.6445	0.6456	0.6467	0.6478
RTVSS	0.5931	0.5943	0.5955	0.5959	0.5964	0.5972

Table 5 highlights the Correlation Coefficient (CC) related with each share generated by the proposed UFCM-PBVC scheme as well as the benchmarked RIVCS and RTVSS approaches. The proposed UFCM-PBVC scheme is determined to ensure superior CC value over the benchmarked RIVCS and RTVSS approaches due to the contextual alternation between Henon map and Lorentz map for ensuring reliable visual cryptographic approach. Thus the CC value of the proposed UFCM-PBVC scheme is determined to be maximized by 6% and 9% predominant over the benchmarked RIVCS and RTVSS approaches.

Table 5: Correlation Coefficient (CC) of the proposed UFCM-PBVC under different shares

The progressive schemes used for comparison	Correlation Coefficient (CC) under different number of shares					
	1	2	3	4	5	6
Proposed UFCM-PBVC	0.9912	0.9908	0.9903	0.9901	0.9894	0.9885
RIVCS	0.9532	0.9527	0.9523	0.9517	0.9513	0.9511

RTVSS	0.9312	0.9301	0.9213	0.9203	0.9201	0.9132

Table 6 highlights the Structural Similarity (SSIM) of each of the shares generated by the proposed UFCM-PBVC scheme as well as the benchmarked RIVCS and RTVSS approaches. The proposed UFCM-PBVC scheme is determined to ensure better SSIM value over the benchmarked RIVCS and RTVSS approaches, since the integration of Hennon map and Lorentz map aided in utilizing the potential features of a chaotic map in an optimal manner. Thus the SSIMvalue of the proposed UFCM-PBVC scheme is determined to be maximized minimized by 8% and 11% predominant over the benchmarked RIVCS and RTVSS approaches.

Table 6: Structural Similarity (SSIM) of proposed UFCM-PBVC under different shares

The progressive schemes used for comparison	Structural Similarity (SSIM) under different number of shares					
	1	2	3	4	5	6
Proposed UFCM-PBVC	0.9821	0.9811	0.9804	0.9796	0.9787	0.9778
RIVCS	0.9623	0.9634	0.9643	0.9652	0.9663	0.9672
RTVSS	0.9521	0.9532	0.9543	0.9552	0.9562	0.9582

5. Conclusions

The proposed UFCM-PBVC technique is contributed as a reliable attempt for enhancing the possibility of preventing the leakage and destruction of sensitive information during the process information exchange and encryption. The UFCM-PBVC technique also included the characteristics of Henon and Lorentz maps for facilitating potential encryption through the derivation of non-linear behavior that results towards the process of efficient sequence generation attributing towards the prevention of information leakage. This proposed UFCM-PBVC technique is determined to confirm a superior entropy of 21.42% and 25.32% predominant over the benchmarked RIVCS and RTVSS approaches. Further, the proposed UFCM-PBVC technique is determined to confirm a minimized MSE of 13.22% and 14.51% predominant over the benchmarked RIVCS and RTVSS approaches. Furthermore, the PSNR value of the proposed UFCM-PBVC technique was confirmed to be reduced by 13.21% and 14.51% excellent to the benchmarked RIVCS and RTVSS approaches.

References

[1] Kaur, H., & Ojha, A. (2016). A Novel Visual Secret Sharing Scheme Using Affine Cipher and Image Interleaving. Advances in Intelligent Systems and Computing, 1(1), 71-80.

[2] Fang, W. (2008). Friendly progressive visual secret sharing. Pattern Recognition, 41(4), 1410-1414.

[3] Uno, K., Hoa, H., & Dung, T. (2015). Visual Secret Sharing by Speckle Pattern Illumination. Proceedings of The 3rd International Conference on Intelligent Systems and Image Processing 2015, 1(1), 67-78.

[4] Chen, Y., Huang, B., & Juan, J. (2018). A (k, n)-Threshold Progressive Visual Secret Sharing without Expansion. Cryptography, 2(4), 28.

[5] Hou, Y., Quan, Z., Tsai, C., & Tseng, A. (2013). Block-based progressive visual secret sharing. Information Sciences, 233(1), 290-304.

[6] Chiu, P., & Lee, K. (2016). An XOR-based progressive visual cryptography with meaningful shares. 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), 1(1), 45-56.

[7] Shivani, S., & Agarwal, S. (2016). VPVC: verifiable progressive visual cryptography. Pattern Analysis and Applications, 21(1), 139-166.

[8] Shivani, S., Agarwal, S., & Suri, J. S. (2018). Development of Visual Cryptography Approaches with Computation Based Recovery of Secrets. Handbook of Image-Based Security Techniques, 1(1), 107-141.

[9] Pandey, D., Rawat, U. S., & Kumar, A. (2016). Robust progressive block based visual cryptography with chaotic map. *Journal of Discrete Mathematical Sciences and Cryptography*, *19*(5-6), 1025-1040.

[10] Pandey, D., & Rawat, U. S. (2016). Chaotic Map for Securing Digital Content. International Journal of Rough Sets and Data Analysis, 3(1), 20-35.

[11] Wu, X., & Sun, W. (2013). Improving the visual quality of random grid-based visual secret sharing. Signal Processing, 93(5), 977-995.

[12] Guo, T., Liu, F., & Wu, C. (2013). Threshold visual secret sharing by random grids with improved contrast. Journal of Systems and Software, 86(8), 2094-2109.

[13] Amiri, T., & Moghaddam, M. E. (2015). A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images. Multimedia Tools and Applications, 75(14), 8527-8543.

[14] Yan, X., Liu, X., & Yang, C. (2015). An enhanced threshold visual secret sharing based on random grids. Journal of Real-Time Image Processing, 14(1), 61-73.

[15] Zeng, Y., & Chang, W. (2016). Inference of Share Stacking Based on Progressive Visual Cryptography. 2016 International Computer Symposium (ICS), 1(1), 56-65.

[16] Shivani, S., & Agarwal, S. (2016). Progressive Visual Cryptography with Unexpanded Meaningful Shares. ACM Transactions on Multimedia Computing, Communications, and Applications, 12(4), 1-24.

[17] Yan, X., Wang, S., & Niu, X. (2015). Threshold progressive visual cryptography construction with unexpanded shares. Multimedia Tools and Applications, 75(14), 8657-8674.

[18] Anila, T., & Wilscy, M. (2013). An Extended Region Incrementing Visual Cryptography Scheme Using Unexpanded Meaningful Shares. Mining Intelligence and Knowledge Exploration, 2(2), 340-349.
[19] Goswami, A., Mukherjee, R., & Ghoshal, N. (2017). Chaotic Visual Cryptography Based Digitized Document Authentication. Wireless Personal Communications, 96(3), 3585-3605.
[20] Merabet, N. E., & Benzid, R. (2018). Progressive image secret sharing scheme based on Boolean operations with perfect reconstruction capability. Information Security Journal: A Global Perspective, 27(1), 14-28.