AN ENHANCED DUAL – IMAGE COMPRESSION AND ENCRYPTION ALGORITHM FORMED ON ARBITRARY PIXEL EXCHANGING

Lijin T V(lijint.v2018@vitstudent.ac.in),
Dr. Deebak B D (deebak.bd@vit.ac.in)

School of Computer Science and Engineering

Vellore Institute of Technology, Vellore

Abstract

Because of the accessibility along with the expanded handling of applications based on multimedia, characteristics as safety measures and that of compression gathered a huge consideration, hence to improve the secrecy along with the strength of dual image encoding models, a dual-image compression and encoding scheme are put forward through merging co-sparse illustration and arbitrary exchanging of pixels. At the start, two clear text images are taken and scrambled this is then represented using the co-sparse study model with matrices having diverse row scrambled. The obtained co-sparse illustration are then exposed to compression and pursued by the encoding close by utilizing compressive sensing. At that point, the resultant estimations gained are inspected and handled by applying the arbitrary pixel exchanging operator pursued by the Arnold transform. At last, the resultant result acquired is joined to frame a total picture and afterward the developed picture is again encoded utilizing the discrete fractional angular transform to enhance and escalate reliability of the total algorithm.

Keywords : *Dual image encryption, DFAT, Arnold transform*

1. Introduction

Protected channeling and the depository of multimedia content are of immense worry in the proliferating digital era purely based on multimedia. Applications which are purely based on multimedia such as surging images require a huge range for their communication. As a result, the collective usage of compression and encoding is very helpful for this kind of such real-time applications. So, the considered encoding algorithm is supposed to be considered strong enough to defend against the assaults. As the demand for safe online depository and channeling of images and film has been witnessing considerably rapid growth in the preceding few decades. Image data protection is very crucial in trouncing pictographic information from practised adversaries. Image encoding is one among those most discussed subjects in the sphere of the image processing. To confirm that the confidential novel image data is not disclosed to attackers, a variety of image encoding steps have been formulated using different techniques, but to an extent majority of them are just meant to change the clean text images into the grained or noised unintelligible form of images. If the volume of the unintelligible image goes beyond that of the pure clean text image, then it would be requiring additional transmission bandwidth and extra storage room, which would be very inconvenient for real-time applications. Therefore, there comes a crucial need to build up a plan to conquer image compression and encoding contemporaneously. So, Compression sensing has pulled in across the board consideration as of its procurement in the sphere of image compression [1].In the preceding few years, numerous image encoding stratagem combining Compression Sensing with that of the other proficient encoding techniques have been introduced. For example, a Compression Sensing hinged on advanced image encoding stratagem focused on block Arnold scrambling and bitwise XOR procedure was put forward to defend against a range of frequent assaults.

1.1 Motivation

Security of images is very crucial in the present internet world. Majority of the available image encoding framework is focused mainly on a solitary image, which is considered unreliable for real-life requirement. Also, a tremendous figure of the image encoding frameworks existing have a reasonable protection performance against assault, but, almost all of them have a frequent downside that the utilization of key is considerably very hefty because the entire measurement matrix in Compression Sensing is considered to be the key. To eliminate this drawback, we design an enhanced dual-image compression and encoding algorithms which use a co-sparse representation with arbitrary pixel exchanging.

1.2 Contribution

Image encryption is one among the extremely remarkable and essential method to protect image data. Image and textual data have their own peculiar distinct features. The encryption algorithms which are present today are just excellent for text data. They might be inappropriate for multimedia data. But most of the present day encryption focuses on single image encryption and it does not fulfil the real-time needs. So, in order to facilitate present-day needs we work on dual image compression and encryption wherein initially two images will be scrambled and represented using co-sparse representation, this would be considered as intermediate cipher text, this co-sparse representation is then compressed and encrypted, then the measurement matrix is evaluated and random pixel operation is performed followed by Arnold transformation, then the images are merged to form an enlarged one which is then subjected to encryption using DFAT [2]. Mainly we make use of compression sensing, Discrete Fourier Angular transform and Arnold transform in our system.

2. Related Work

Xing Yuan Wang et.al [3] in his paper used a method which was based on iterating chaotic maps that exhibit some kinds of chaotic behaviour. The proposed system used the pseudorandom sequence which was formulated with the help of a set of 1-D chaotic maps. The above-mentioned algorithm guarantees rapid encoding and the decoding of both the monochromatic image and the true colour image. It also provides the user with a flexible privilege to set the number of rounds of encryption. As it provides the user with the privilege to set the rounds of encryption, as the integral number of encoding rounds proliferate, the dispensation speed decreases.

Amitava Nag et.al [4] in his work he adopted a method of affine transformation on the plain text image followed by XOR operation on the resulting image. They proposed a system which basically focused on location transformation based encryption technique. It shuffles the values of the pixel to the disparate location by utilizing the properties of affine transform technique. The image which is transformed is then separated into 2x2 blocks of the pixel and each of the blocks is subjected to be encrypted using XOR. It used 64 bits key. Though the proposed system is Lengthy, complicated and chances of mistakes are high.

Seyed Hossein Kamali et.al [5] in his research he focused on modifying the AES algorithm by manipulating the shift row transformation. The author proposed a refinement to the existing AES to achieve distinctive security and more reliable better image encoding. The refinement is the algorithm is generally performed by calibrating the shift-row transformation. The algorithmic program and therefore the secret key consequently has the same information that is ciphered to an equivalent value which is the main security weakness.

Huijuan Li, et.al [6] designed a novel technique which formulated on the discrete DFRT and the chaotic maps (CM). The arbitrary matrices utilized by DFRT are created by making use of a CM.

Anyone among the available two novel images is jumbled by using a different CM which is further encoded into the segment of a composite matrix with the other novel image as its amplitude. Then this composite matrix is encoded by the DFRT. On applying the right keys that incorporates the preliminary values, control parameters, and abridged positions of the CM, and fractional orders, the two novel images can convalesce with no cross-talk.

Zhu Yu et.al[7] in his work proposed a method which used Wavelet Transform (WT) to develop a Chaos Based Image Encoding Algorithm, in the work he presented uses the scheme uses the wavelet decomposition focusing on image data in the soaring-frequency sub-band image, and then encoding is employed for the sub-band image. After WT is instigated in order to spread the encoded portion all over the entire image. Another encoding method is employed to wind up the encoding procedure.

3. Proposed Methodology

Inorder to encourage present-day needs we take a shot at dual picture compression and encryption wherein at first two pictures will be mixed and spoke to utilizing co-sparse representation, this would be considered as moderate figure message, this co-sparse representation is then packed and scrambled, at that point the estimation network is assessed and arbitrary pixel operation is performed trailed by Arnold transform, at that point the pictures are consolidated to shape an expanded one which is then exposed to encryption utilizing DFAT . For the most part we utilize compression sensing, Discrete Fourier Angular change and Arnold transform in our framework.

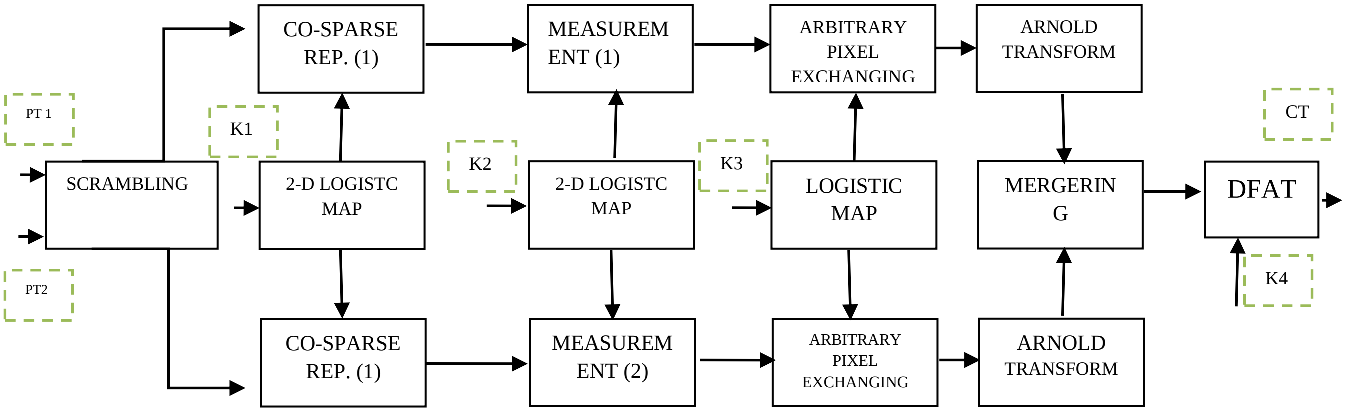

FIG 1 Encryption Phase

The above block diagram illustrate the process of compression and encryption, in this phase we initially accept two clear text images which are then subjected to scrambling and then this scrambled clear text image is represented in the form of co-sparse representation model upon which these co-sparse representations are exposed to 2-D logistic mapping with initial values x_0 and y_0 which is reiterated to acquire arbitrary sequence of x and y. Here x_0 and y_0 are considered as K1. Two matrices are formed and rows of these matrices are reorganized in proportion to the rising sort of x and y, and two matrices are obtained with rows scrambled. Then a measurement matrix is formed using the key as x_0' and y_0' (K2). Then the logistic map is reiterated $\sqrt{M}$ times with initial value z (K3) to acquire arbitrary chain of z. Further, the arbitrary pixel exchanging is performed. After the arbitrary pixel exchanging is done it is then subjected to Arnold transformation and the ensuing images are combined in the horizontal fashion to produce an enlarged complete image. This enlarged image is re-encoded using DFAT [6] to enrich the reliability of the entire scheme.

The underneath block diagram delineates the procedure of decompression and decryption; this is the invert procedure of the previously mentioned compression and encryption process. The CT is at first processed by IDFAT then the outcome is isolated into two equivalent amounts of the even way and with the assistance of ART and IAPE, two square frameworks are segregated.The obtained square networks are then converted over to 1-D vectors and the decoded pictures PT-1 and PT-2 are reestablished by the assistance of the SBI algorithm.

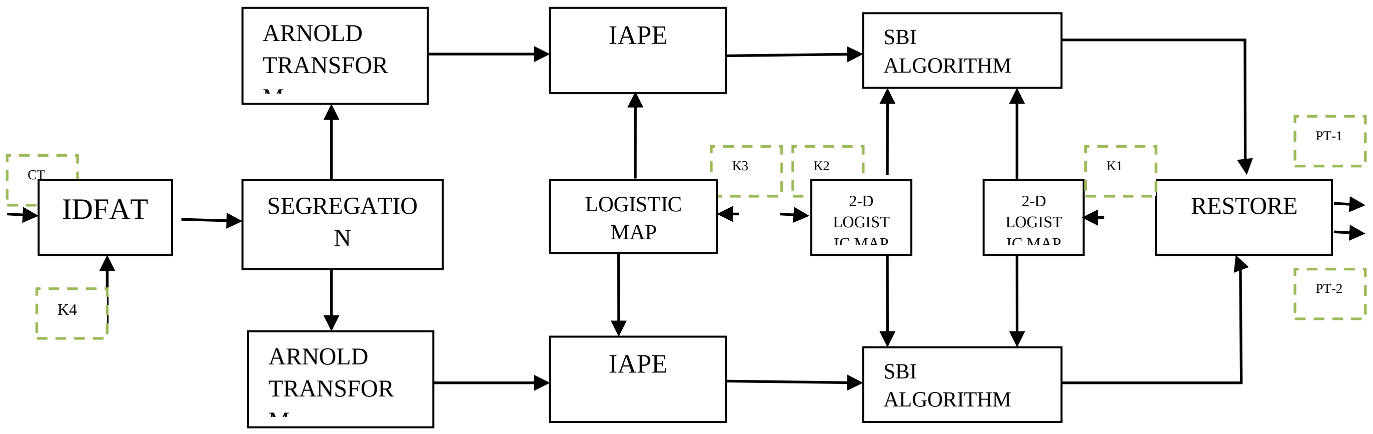

FIG 2 Decryption Phase

4. Discussion

S.NO	AUTHOR	TECHNIQUE PROPSED	CHALLENGES ADDRESSED
1.	Sui Liansheng et. al [9]	To give the expanded arbitrariness a multiple image encoding model using the nonlinear iterative stage recuperation scheme in the gyrator transform space under the enlightenment of an optical vortex beam is prescribed.	With the utilization of the untidy composed phase mask, the issue of pivot arrangement in the optical setup can undoubtedly be redressed.
2.	Zhengjun Liu et. al [10]	They consolidated Arnold transform and DFAT to define a dual image encoding. They enchanced the security by using the parameters of the two changes which they utilized as an extra key.	The Arnold transformation would be carried out quite a surplus number of times. Produces a very complex output and consumes a large computation power.
3.	Zhou Bei et. al [11]	The author focused on formulating an optical color image watermarking model taking in consideration of the human visual characteristics and the same is presented to the gyrator transform space.	They could recreate the watermark with exceptionally lofty perceptual quality and furthermore could improve the security angles by having an extensively high affectability to the secret keys.
4.	Xianye Li et.al [12]	In light of row scanning compressive imaging and phase recovery from Fresnel space they	It utilizes various systems in every iterations which needs a powerful utilization. Sub key age and

		built up a multi-picture encryption strategy.	reproduction of the equivalent amid decoding, makes it progressively perplexing.
5.	Ch.K. Volos et. al [13]	Technique like chaotic genuine arbitrary piece generator which will synchronize phenomena at the point of image encoding. In this initial one is chaotic synchronization and second one is backwards phi-lag synchronization.	The major thing when the bit stream is generated by the TRBG it is used to encrypt the gray scale images with XOR operation.
6.	M.Y.Mohamed Parvees et. al [14]	For encoding they utilized 16 bit grayscale advanced picture which can be upgraded by the chaotic financial map.	At the point when the pixels get mixed to build the pixel proficiency they did stage, substitution process then the framework will get more buildings.
7.	R. Prem Kumar et al.[15]	They utilized strategy named secure and compound chaos based image encoding. For scrambling the picture they utilized a mystery key with half and half tasks. They broke down on 3D pictures since they can accomplish greater security and strength for the pictures. Indeed, even those pictures are dark scale pictures.	In chaos map traverse and transformation is the vital stage. The information pictures are scrambled by the hybrid and they are declined into bit planes. We can swap the bit fields by utilizing numerous hybrid tasks. Here the scrambled picture is acquired by the change procedure. At last they accomplished high security in power.
8.	Chong Fu et al.[16]	Chaos based image encoding method is used in which gray scale replacement is done using	By the mix of permutation and substitution tasks they made the encoding model solid which is

		circular bit shift method. By this they improve more security. This chaos provides less security and it is sensitive.	against to known and picked plain content assaults. The significant favorable position the key space is expanded and binary, decimal key streams have great properties which improves the security.

5. Conclusion

An enhanced dual-image compression and encoding method formed on co-sparse illustration and arbitrary exchanging of pixel are studied. Arbitrary sequences were utilized for shuffling the DCT dictionary rows and initial row vectors of the circular dimension matrices in CS are formulated by 2D-Logistic map, individually. Initially two clear text images are taken which are then scrambled and depicted by the co-sparse representation scheme with various rows shuffled dictionaries and obtained output is encoded by help of CS. The arbitrary exchanging of pixels and the Arnold transform is utilized for swapping over the pixel position of selected encoded images, wherein the decision matrix is superintended by Logistic map. Further, the evolved images are combined collectively in the horizontal fashion and then re-encoded using DFAT

REFERENCES

[1] Donoho DL . Compressed sensing. IEEE Trans Inf Theory 2006;52:1289–306

[2] Liu, Z., Ahmad, M.A. and Liu, S., 2008. A discrete fractional angular transform. *Optics Communications*, *281*(6), pp.1424-1429

[3] Wang, X., Zhao, J. and Liu, H., 2012. A new image encryption algorithm based on chaos. *Optics Communications*, *285*(5), pp.562-566.

[4] Nag, A., Singh, J.P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D. and Sarkar, P.P., 2011, July. Image encryption using affine transform and XOR operation. In *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies* (pp. 309-312). IEEE.

[5] Kamali, S.H., Shakerian, R., Hedayati, M. and Rahmani, M., 2010, August. A new modified version of advanced encryption standard based algorithm for image encryption. In *2010 International Conference on Electronics and Information Engineering* (Vol. 1, pp. V1-141). IEEE.

[6] Li, H. and Wang, Y., 2011. Double-image encryption based on discrete fractional random transform and chaotic maps. *Optics and Lasers in Engineering*, *49*(7), pp.753-757.

[7] Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P. and Yunpeng, Z., 2010, March. A chaos-based image encryption algorithm using wavelet transform. In *2010 2nd International Conference on Advanced Computer Control* (Vol. 2, pp. 217-222). IEEE.

[8] Liu, Z., Ahmad, M.A. and Liu, S., 2008. A discrete fractional angular transform. *Optics Communications*, *281*(6), pp.1424-1429.

[9] Liansheng, S., Bei, Z., Xiaojuan, N. and Ailing, T., 2016. Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. *Optics express*, *24*(1), pp.499-515.

[10] Liu, Z., Gong, M., Dou, Y., Liu, F., Lin, S., Ahmad, M.A., Dai, J. and Liu, S., 2012. Dual image encryption by using Arnold transform and discrete fractional angular transform. *Optics and Lasers in Engineering*, *50*(2), pp.248-255.

[11] Liansheng, S., Bei, Z., Zhanmin, W. and Ailing, T., 2017. An optical color image watermarking scheme by using compressive sensing with human visual characteristics in gyrator domain. *Optics and Lasers in Engineering*, *92*, pp.85-93.

[12] Li, X., Meng, X., Wang, Y., Yang, X., Yin, Y., Peng, X., He, W., Dong, G. and Chen, H., 2017. Secret shared multiple-image encryption based on row scanning compressive ghost imaging and phase retrieval in the Fresnel domain. *Optics and Lasers in Engineering*, *96*, pp.7-16.

[13] Volos, C.K., Kyprianidis, I.M. and Stouboulos, I.N., 2013. Image encryption process based on chaotic synchronization phenomena. Signal Processing, 93(5), pp.1328-1340.

[14] Pareek, N.K., Patidar, V. and Sud, K.K., 2006. Image encryption using chaotic logistic map. Image and vision computing, 24(9), pp.926-934.

[15] Premkumar, R. and Anand, S., 2018. Secured and compound 3-D chaos image encryption using hybrid mutation and crossover operator. Multimedia Tools and Applications, pp.1-17.

[16] Fu, C. and Zhu, Z., 2008, November. A chaotic image encryption scheme based on circular bit shift method. In 2008 The 9th International Conference for Young Computer Scientists (pp. 3057-3061). IEEE.

[17] Zhou, N., Jiang, H., Gong, L. and Xie, X., 2018. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Optics and Lasers in Engineering*, *110*, pp.72-79.

[18] Maan, P. and Singh, H., 2018. Non-linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain. *3D Research*, *9*(4), p.53.

[19] Zhu, R., Li, G. and Guo, Y., 2019. Compressed-Sensing-based Gradient Reconstruction for Ghost Imaging. *International Journal of Theoretical Physics*, pp.1-12.

[20] Gong, L., Qiu, K., Deng, C. and Zhou, N., 2019. An image compression and encryption algorithm based on chaotic system and compressive sensing. *Optics & Laser Technology*, *115*, pp.257-267.

[21] Wu, C., Wang, Y., Chen, Y., Wang, J. and Wang, Q.H., 2019. Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain. *Optics Communications*, *431*, pp.203-209.

[22]Singh, S. and Majumdar, A., 2017. Analysis co-sparse coding for energy disaggregation. *IEEE Transactions on Smart Grid*.

[23] Zhou, N., Yan, X., Liang, H., Tao, X. and Li, G., 2018. Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. *Quantum Information Processing*, *17*(12), p.338.

[24] Sui, L., Duan, K. and Liang, J., 2015. Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. *Optics Communications*, *343*, pp.140-149.

[25] Huang, H. and Yang, S., 2016. Colour image encryption based on logistic mapping and double random-phase encoding. *IET Image Processing*, *11*(4), pp.211-216.