An Efficient Encoding Technique based on Chaotic Cryptography for Digital Image

Deepak Kourav, Taslima Ahmed, Prashant Mavi

Abstract: Presently advanced India notoriety, associations are proposing various structures concentrating on computerized encoding procedures. Because of the simplicity of replicating, altering, and altering of computerized archives and pictures has prompted encoding the data required for transmission and capacity. It clear that the connection between's the picture pixels to its neighborhood district is high, decreasing relationship between's the pixels esteem makes it hard to figure for the first picture and along these lines enhance the security. This paper presents a novel picture encoding strategy which at first improves the picture based on exchanging dim codes and pixel blast. The pixel blast utilizes very much characterized key that switches between the dim code of the picture pixels. Exploratory outcomes would demonstrate that the proposed pixel blast is sufficient for fractional encoding and upgrades security of the information. Further, it could likewise bolster as a deadly implement for any current calculation.

Index Terms: Encoding, Gray-Code, Pixel Blast, Authentication

I. INTRODUCTION

As the computerized India is picking up the force, the security related with advanced archive and pictures is turning into a functioning examination zone. What's more, quick improvements in the cutting edge correspondence framework have permitted the exponential ascent in information exchange over the system easily. Presently a-days, it obvious and reported that there is a critical ascent in the privacy rupture of certain touchy information because of increment in the quantity of aggressors. By and large, the greater part of the assailants center around abusing mystery data as the exchange of information and data occur through web is of high volume. As it is open-community channel constraining the entrance would hamper the execution and dependability of the channel. Subsequently to balance this powerlessness, numerous specialists have thought of productive calculations to scramble the computerized data before transmission and capacity in open-free channels.

Encoding is a science that arrangements with the change of information into a frame that is disjointed to any watcher without the proper learning (a key or code) [1]; truly it changes plain content into figures.

Encoding is the exploration of utilizing science based change to encode or decode the information. Encoding is utilized to keep information from the unapproved get to which decreases the likelihood of unapproved get to a few times and just the approved work force's having the key is permitted to get to it. The essential consideration has now moved towards upgraded and secure correspondence.

From these the data security is most driving territory of research. The framework in any condition ought to be sufficiently secure to limit any sort of unapproved get to and just the approved work force should just be permitted to get to the data. Because of the absence of the suitable security method, data security has turned into a colossal issue. The picture encoding component should characterized to such an extent that the encoded picture will just changed over back to the plain picture at collector end by approved staff with key [2]. Likewise, the recreated picture must be lossless. Pixel connection is the connection of the pixel to its encompassing pixel esteems that should be tended to while characterizing the encoding work. Different encoding motors which guarantee extremely upright encoding approach for scrambling mixed media. The majority of them are known in particular RSA [3], DES [4] and so forth. They scrambling literary information however to the extent the picture encoding is concerned it utilizes more space and take additional time due to mass picture information (pixel esteems) in all the three layers. It ought to be noticed that these encoding and unscrambling activities are guided by some particular keys, where the keys might be same or can be effortlessly gotten from the learning. Such cryptographic procedures are gathered under private key cryptography [5], [6]. On the other hand, encoding and decoding keys might be unique or it may not be doable to determine one key despite the fact that the information of other key is accessible, and such cryptographic strategies are known as open key cryptography [4]. An all around characterized encoding ought limit the relationship between's the pixels as well as sufficiently quick to execute rapidly while encoding information. What's more, the great encoding plan ought to give both protection and security and is lossless in nature. It ought to be sufficiently extreme to have insusceptibility against cryptanalysis and has a multi target issue limiting the relationship affect among the pixels. So it is vital to diminish the connection between's the encompassing pixels and increment the level of irregularity of the picture. However, it can't stop an insider (worker, doctor, merchant, business accomplice, and so forth.) to get to the secret data.

Present day encoding motors are upgraded by different current methodologies anyway there are a few methodologies which naturally have distinctive qualities and thus clashing connection held among them.

Manuscript received on May 25, 2020.
Revised Manuscript received on June 29, 2020.
Manuscript published on July 30, 2020.

* Correspondence Author
Dr. Deepak kourav, Associate Professor, IIMT College of Engineering Greater, Noida UP, India.
Dr. Taslima, Associate Professor, IIMT College of Engineering Greater, Noida UP, India.
Mr. Prashant Mavi, Associate Professor, IIMT College of Engineering Greater, Noida UP, India.

In this paper, we propose a novel calculation that aides in lessening the connection among the pixel by utilizing exchanging dark code components which will additionally improve the security of the cover picture. The proposed strategy considers the entire picture as one to work upon, we cut the picture into different cuts on a level plane and vertically and moving them which will additionally decreases relationship and henceforth increment encoding record.

What's more, we actualize a straightforward changing philosophy to upgrade the crypto benefits against cryptanalysis systems. The method is executed on the current Riotous cryptography Bit Plane Disintegration Calculation [2] and the outcomes are observed to be made strides. Additionally, there are no adjustments on the aggregate size of picture amid encoding and decoding process. Whatever is left of this paper is sorted out in following way. In Segment 2, we present the current confused cryptography based deterioration and propose a novel technique which will work upon the current one. Area 3 presents the new approach equation where the cutting edge dark code exchanging calculation has been actualized. Area 4 manages proposed framework structure and the essential advances utilized. Segment 5, incorporates the recreations comes about related with proposed calculation. The finish of the paper is displayed in the area 6.

II. BACKGROUND

In this segment, a detail study on existing computerized picture control calculations that are promptly accessible for advanced encoding is displayed. It is exceptionally easy to alter any picture and make it accessible to others by exhibiting proprietorship, validation evidence. In this manner fore, protecting computerized media uprightness has along these lines turn into a noteworthy worry among the specialists in the current advanced time. Encoding is a standout amongst the most well-known methods for consolidated by associations as device for trustworthiness requirement, anchored correspondence, altered confirmation channel and verification. In this paper, we exhibit a novel picture encoding strategy which at first adjusts the picture based on exchanging dim codes and pixel blast at that point completes existing encoding calculations. Contrasted with the systems and conventions for security generally utilized to play out this undertaking, a specific accentuation on connection between's the neighbor-hood pixels.

Some productive ways are proposed by Mayhem based cryptographic calculations to create secure picture encoding procedures. A picture encoding in view of hyper-turbulent guide meets the necessities of the safe picture exchange. The ergodic grid of one hyper-confused arrangement is utilized to permute picture, the type of which is chosen by a disorderly calculated guide, the other hyper-clamorous succession is utilized to diffuse permuted picture. To make the figure more strong against any assault, we need to process a few rounds of change and dispersion. The underlying states of the hyper-riotous guide are adjusted after each round. The aftereffects of different trial, measurable examination and key affectability tests demonstrates that the proposed picture encoding plot gives a productive, powerful and secure route for picture encoding and transmission [7]. M-Arrangement in light of Picture scrambling parameter can be delivered by a progression of move registers is presented as pseudo encoding calculation. Likewise, the parametric M-arrangement is misused wherein; the client can change the security keys, r, which demonstrates the quantity of executed move tasks , or the separation parameter p, to create a wide range of M-groupings. In this way guaranteeing the mixed pictures are hard to disentangle while offering an abnormal state of security assurance for the pictures. The calculation introduced here can scramble the 2-D or 3-D pictures in a single step. It likewise calculations safe against the picture assaults, for example, information misfortune and commotion assaults [8]. The calculation can be connected in the ongoing applications as it is a direct procedure and can be effortlessly executed.

III. PIXEL EXPLOSION AND SWITCHING TECHNIQUES

In a perfect encoding calculation, the connection between's the two slantingly adjoining, vertically neighboring and on a level plane nearby pixels of the figured picture ought to be low. Further, this strategy could be turned out to be exceptionally solid in blend with the weaker and less secure encoding procedures. In a word, the picture is seen as the blend of the pixels (RGB layers) which is the littlest component of a picture that contains the picture trademark in a segregated frame. These RGB pixel esteems by and large, have high connection with the neighboring pixels because of the progressive change in the picture qualities. Pixel blast is a procedure that spotlights on moving out of the local pixel and moved into some other pixel in existing in the picture limits. Therefore, the relationship between's the pixels in given layer could be limited radically. In this paper, the move utilized and talked about are direct and round. The round move guarantees that there is no loss of information or overwriting of the qualities. The Moving of the qualities depend on specific standards and surmisings from the key gave toward the start of the procedure. This key is fundamental for effective reproduction of the cover picture from its figure and gives crypto benefits against beast constrain assault.

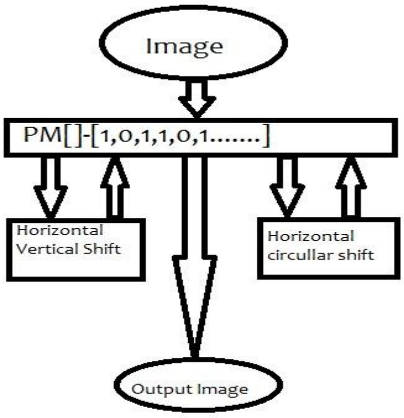
Image
PM[]-[1,0,1,1,0,1.......]
Horizontal Vertical Shift
Horizontal circullar shift
Output Image

Fig 1. Pixel Explosion Scheme [15]

Exchanging hypothesis is an outstanding method utilized in planning clever controllers for rationale controls. Its applications stretch out to different fields of building, bio-innovation, promoting and so on.

The conveyance of the pixels differs starting with one district then onto the next and starting with one neighborhood then onto the next inside a given locale. Existing strategies treat each pixel (expect zero) inside a square with a similar control method.

Consequently, we fused the well exchanging hypothesis into the proposed calculation for underwriting this issue and improve the crypto proficiency and at the same time upgrade its insusceptibility against savage power assault. The least difficult square graph for exchanging system is introduced in the figure 2.

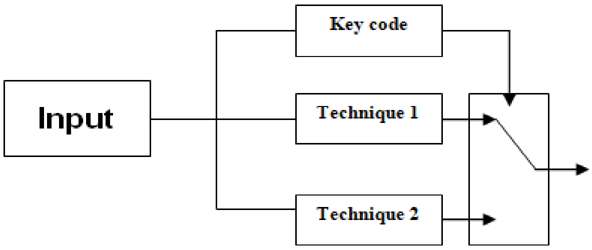

Fig 2. The basic structure of the Switching Mechanism incorporated

The information is information that has fluctuating qualities (such recurrence, repetition parts or and so on). Key-code is parameter that is client characterized which goes about as reason for exchanging between two methodologies. Approach 1 is an instrument that is have to performed under specific limitations and approach 2 is another that is performed in the remaining.

IV. PROPOSED ALGORITHM

To outline an anchored encoding plot, it isn't just imperative to know how to control/change information inside a cover picture yet in addition we have to know how to recreate the first data from controlled/adjusted information of the cover picture. In this area, we introduce in detail the highlights of the proposed encoding calculation for computerized pictures in view of pixel blast and exchanging dark code encoding. Moreover, we likewise clarify about connection based connection between the picture sub-squares and control information bit for fruitful recreation of encoded information. The proposed calculation could adequately remake the scrambled data lossless with approved learning of the keys related amid the encoding of unique cover media. The Fig.3 presents a detail square outline of encoding and decoding procedure of the proposed calculation.

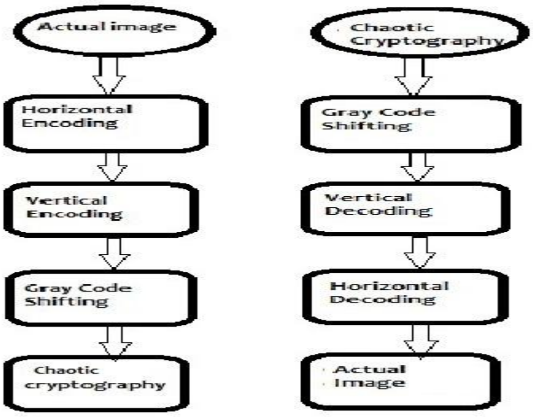

Fig 3. Block Diagram of Encoding and Decoding Process of the proposed algorithm

As we can see in the block diagram in figure 3, the correlation effect within the cover picture can be minimize by either column-wise pixel explosion or row-wise pixel explosion with the help of vertical &horizontal block displacement. As discuss in previous section that direct encoding can maintain the correlation factor for similar lines, which might be suitable for modern encoding techniques. So the proposed encoding method encodes the data in such a way that it can be retrieved without the use of knowledge keys incorporated for encoding process. In this method we have shown a specific relation of pixel explosion using switching mechanism in which the gray-code mechanism is used for alteration of key based pixels and other pixels are remain unaltered so the boosting of crypto benefits.

A. Steps in Encoding Technique

Input: The data which need to be encoded
Step1: Select the key-code for pixel explosion
Step2: Break up the cover image into different rows. Now based on switching and key-code divide rows into unchanged and gray-code.
Step3: Break up the cover image into different columns. Now based on switching and key-code divide columns into unchanged and gray-code.
Step4: Convert the encoded data into a string of the binary bits, now convert the every bit into gray-code, and adjoin to encoded stream.
Step5: Reconstruct the image blocks using encoded string of bits.
Step6: Determine the encoding that can be incorporated over the uncorrelated bits encoding algorithm.
Output: Get the encoded image.

The main aim of any encoding system is to obtain a high un-correlation between the neighborhood pixels in the cover image. So, we can shuffle data randomly before manipulating the data based on key that could transferred with the image or externally.

B. Decoding Algorithm

Procedure of decoding is very simple and it is nothing but the reverse process of encoding. The required steps for decoding are as follows:

Input: Take Crypto image as input
Step1: Crypto image decomposition in to different binary steam based on the key.
Step2: Represent gray-code of bit by binary code now construct digital image using binary bits.
Step3: Recover the cover image by different columns after differentiates columns into unchanged and gray-code based switching and key-code.
Step4: Recompose the cover image through various rows after differentiates rows into unchanged and gray-code based switching and key-code.
Step5: Recombine the reconstructed binary information
Output: Output the reconstructed cover image.

The cover image that has been reconstructed has no distortion from the original image. The integrity of the system can be improved by switching gray code and pixel explosion process as encoding process.

V. COMPUTER SIMULATIONS AND RESULTS

In this section, the simulation and results of proposed method of encoding is presented in detail. We have used MATLAB software for computer simulation. Analysis of images done by varying different parameters size of image, type of image and class of image. These images are stored as uncompressed TIFF image some of them where converted into bitmap images by threshold.

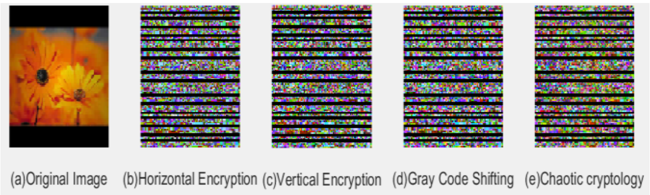

Fig.4 a) Original image of Flower b) Horizontal encoded, c) Vertical encoded, d) Gray-code shifting e) Encoded image

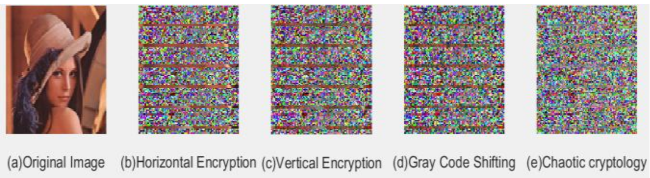

Fig.5 a) Original image of Lena b) Horizontal encoded, c) Vertical encoded, d) Gray-code shifting e) Encoded image

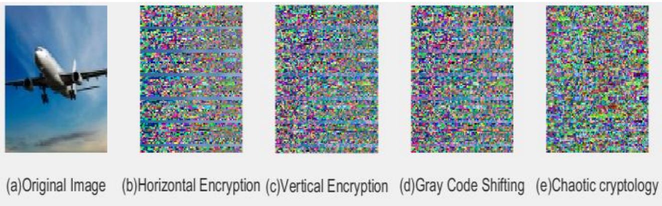

Fig.6 a) Original image of Airplane b) Horizontal encoded, c) Vertical encoded, d) Gray-code shifting e) Encoded image

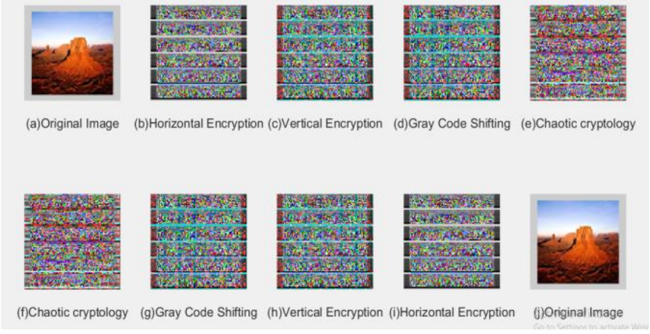

Fig.7 a) Original image of Desert b) Horizontal encoded, c) Vertical encoded, d) Gray-code shifting e) Encoded image after Chaotic cryptography f) Chaotic cryptography encoded image g) Decoded image (gray-code shifting) h)Vertically decoded image i) Horizontally decoded image and j) Decoded original image

In this section we have check first order statistics by comparison of histogram of encoded and decoded image. Fig. 8 and 9 shows the histogram of encoded and decoded images respectively.

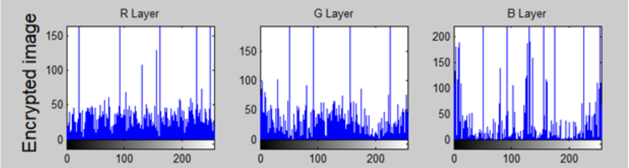

Fig.8 The histograms of RGB layers of the Encoded image "Desert"

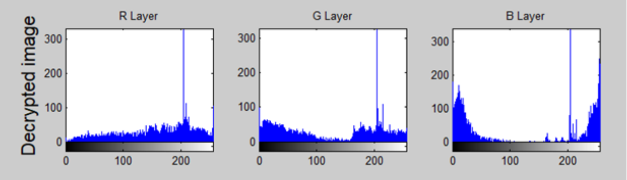

Fig.9 The histograms of RGB layers of the Decoded image "Desert"

In this work, we have also done comparison between various image features which shows the feasibility of the proposed algorithm to various types of encoding algorithms as illustrated in table 1, table 2. Percentage pixel change in each layer of 'DESERT'

Shift Code	Chaotic cryptography Bit Plane Decomposition Algorithm			Proposed Algorithm		
	R	G	B	R	G	B
1	49.624	56.5223	53.5231	33.15	34.26	32.33
2	67.1427	72.3127	68.414	33.26	32.16	32.29
3	85.4215	88.6219	74.9217	34.19	31.57	32.35
4	84.2415	88.2546	72.8512	33.28	32.17	33.15
5	81.4372	84.5833	82.1263	33.17	34.20	33.15
6	74.5427	78.4550	83.9243	32.25	33.17	32.45
7	63.1482	75.3258	79.5624	32.24	34.08	33.27
8	59.2221	76.8451	78.1398	32.24	33.20	32.24
9	62.4811	78.6448	76.7534	33.27	34.12	33.27
10	64.3549	81.4568	79.7146	34.18	32.20	33.25
11	78.1054	86.7642	84.7129	32.27	33.15	32.24

TABLE I. **Correlation Between Pixel**

Images	Original Image	Encoded Image
Lena.jpg	0.4217	0.4023
Flower.jpg	0.1024	0.0969
Desert.jpg	0.1322	0.0993
Airplane.jpg	0.0958	0.0908
Desert.png	0.1132	0.0868

In the above test we have perceived that the proposed framework could furnish compelling encoding in examination with the current calculation. The table I to table III shows information demonstrates pixel change for each layer for a portion of the move code for different pictures. Likewise the relationship is decreased to min estimation of 0.0889 for "airbus.jpg" which indicates most extreme bending between the cover and figure picture. Moreover, the assailant may utilize the savage power assault that attempts all conceivable mix to develop the ideal ace picture.

VI. CONCLUSION

In this paper, we presented a novel picture encoding strategy which at first adjusts the picture based on exchanging dim codes and pixel blast. The reenactment comes about demonstrate that exchanging dim code and pixel blast essentially diminishes the connection affect inside the area while encoding the cover picture. It is apparent that this structure could be utilized for fractional encoding progressively applications and recordings. The pixel blast utilizes very much characterized key that switches between the dim code of the picture pixels. Along these lines, the proposed calculation upgrades security of the cover data. Further, test comes about demonstrates that the proposed pixel blast is sufficient for fractional encoding and improves security of the information. Furthermore, it could likewise bolster as a deadly implement for any current calculation.

REFERENCES

1. Xinyi Zhou, 2Wei Gong, 3WenLong Fu,LianJing Jin “Improved Method for LSB Based Color Image steganography Combined with Cryptography”. IEEE 2016
2. C. C. Ravindranath, Bhatt A K and Bhatt A; “Adaptive Cryptosystem for Digital Images using Chaotic cryptography Bit- Plane Decomposition” International Journal of Computer Applications (0975 – 8887)Volume 65– No.14, March 2013
3. RSA Security. http://www.rsasecurity.com/rsalabs/faq/3-2-6.html
4. DES. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. The urlexplains the concept of the Data Encoding Standard.
5. S. S. Maniccam and N. G. Bourbakis,“Image and video encoding using scan patterns,” Pattern Recognition 37, pp. 725-737, 2004. NJ: Prentice Hall, 2003
6. B. Furht, D. Socek, and A.M. Eskicioglu, “Fundamentals of Multimedia Encoding Techniques,” Chapter in Multimedia Security Handbook, pp. 94 – 144, CRC Press, 2005
7. L. C. L. Chuanmu and H. L. H. Lianxi, “A New Image Encoding Scheme based on Hyperchaotic Sequences,” 2007 Int. Work. Anti-Counterfeiting, Secur. Identif., 2007.
8. Y. Zhou, K. Panetta, and S. Agaian, “An image scrambling algorithm using parameter based M-sequences,” in Proceedings of the 7th International Conference on Machine Learning and Cybernetics, ICMLC, 2008, vol. 7, pp. 3695–3698.
9. Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, “Image encoding using P-Chaotic cryptography transform and decomposition,” Opt. Commun., vol. 285, pp. 594–608, 2012.
10. Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, “(n, k, p)-Gray code for image systems,” IEEE Trans. Cybern., vol. 43, pp. 515–529, 2013.
11. J. Z. J. Zou, R. K. Ward, and D. Q. D. Qi, “The generalized Chaotic cryptography transformations and application to image scrambling,” 2004 IEEE Int. Conf. Acoust. Speech,
12. W. Zou, J. Huang, and C. Zhou, “Digital image scrambling technology based on two dimension chaotic cryptography transformation and its periodicity,” in Proceedings - 3rd International Symposium on Information Science and Engineering, ISISE 2010, 2011, pp. 415–418.
13. J. Z. J. Zou, R. K. Ward, and D. Q. D. Qi, “A new digital image scrambling method based on Chaotic cryptography numbers,” 2004 IEEE Int. Symp. Circuits Syst. (IEEE Cat. No.04CH37512), vol. 3, 2004.
14. Y. Zhou, K. Panetta, and S. Agaian, “Image encoding algorithms based on generalized P-Gray Code bit plane decomposition,” in Conference Record - Asilomar Conference on Signals, Systems and Computers, 2009, pp. 400–404.

AUTHORS PROFILE

Dr. Deepak kourav has done his Btech from RGPV, Bhopal he has done MTech from RGPV, Bhopal and Ph.D from Dr. KN Modi University Jaipur. He worked in different engineering colleges and have 12 years of teaching experience. He has published 15 research papers in different journals. Currently he is working as Associate professor in IIMT College of engineering Greater, noida UP.

Dr. Taslima has done his B.tech from jorhat enginereering college and MTech. From Tezpur Uuniversity she has done her Ph.D from Tezpur University. She worked in different engineering colleges and have 12 years of teaching experience. Currently she is working as Associate professor in IIMT College of engineering Greater, noida UP.

Mr. Prashant Mavi has done his B.tech from N.M.U Jalgaon Maharashtra and MTech. From UPTU. He worked in different engineering colleges and have 20 years of teaching experience. Currently he is working as Assistant professor in IIMT College of engineering Greater, noida UP.