An Encryption Algorithm for Enhanced Image Security

Sivaji Satrasupalli, S Vishnu

Abstract—Image security finds its applications in many areas such as bio-metric, digital signatures, watermarking, confidentiality of medical and data in transit. It has become necessary to secure the images in order to protect the confidential data. Cryptography is one of the methodologies through which image data can be secured for storing or transmission purposes by encrypting the same and decrypt it when needed. The main challenge in image encryption is generating cipher which takes less computational without compromising the security. In this paper, we present a symmetric encryption algorithm which outperforms the existing algorithms such as AES, DES, Blowfish and etc which require more computational time on bulk amounts of data.

Index Terms—Cryptography, image security, computational time

I. Introduction

Cryptography is one of the areas in mathematics in which few computations are performed on data for the confidentiality and security. Cryptography comprises of two steps: first is encryption in which computations are performed on the data to be secured and the cipher text is generated. Second is decryption, few computations are performed on the cipher text to generate the original data. To encrypt and decrypt the data, a key is needed. In order to access the encrypted or decrypted by any user, a key is often used. There exist two methods, symmetric and asymmetric encryption based on the usage of this key. Same key is used for both encryption and decryption in the former and different keys called public and private keys are used in the latter.

A decent data security framework cannot just secure confidential messages in the content structure, however likewise in picture structure. When all is said in done, there are three fundamental qualities in the data security field: Privacy, Integrity and Availability ([6]). Data security field as pursues:

1. Privacy: an unapproved client can't reveal a message.
2. Integrity: an unapproved client can't change or corrupt a message.
3. Availability: messages are made accessible to authorized clients dependably.

Nonetheless, pictures are different from content. Despite the fact that we may utilize the customary cryptosystems, (for example, RSA and DES-like cryptosystems) to encode pictures straightforwardly, it is not a smart thought for two reasons. One is that the picture measure is quite often a lot more prominent than that of content. Hence, the customary cryptosystems need much time to straightforwardly encode the picture information. The other issue is that the decoded content must be equivalent to the first content. Be that as it may, this prerequisite isn't important for picture information. Because of the normal for human observation, a unscrambled picture containing little twisting is for the most part worthy[8]. With the tremendous development of computer systems and the most recent advances in computerized advances, a colossal measure of computerized information is being traded over different sorts of systems. Usually obvious that a substantial piece of this data is either secret or private. Thus, various security systems have been utilized to give the required assurance.

Correspondence security of advanced pictures and printed computerized media can be practiced by methods for standard symmetric key cryptography. Such media can be treated as parallel arrangement and the entire information can be scrambled utilizing a cryptosystem, for example, Advanced Encryption Standard (AES) or Data Encryption Standard (DES) [9, 7]. As a rule, when the mixed media information is static (not a continuous gushing) it can treated as an ordinary twofold information and the traditional encryption systems can be utilized. Choosing what dimension of security is required is more enthusiastically than it looks. To distinguish an ideal security level, the expense of the interactive media data to be ensured and the expense of the assurance itself are to be thought about cautiously. Accordingly, insurance of computerized pictures against illicit replicating and conveyance has moved toward becoming a significant issue[10]. Picture encryption strategies endeavor to change over a picture to another one that is difficult to comprehend. Then again, picture decoding recovers the first picture from the encoded one. There are different picture encryption frameworks to encode and decode information, and there is no single encryption calculation fulfills the diverse picture types[11, 12].

II. RELATED WORK

[1] proposed a new scheme called New side-match vector quantizer (NewSMVQ) to improve the quality, encrypting speed, and bit rate to compress the images. They have come up with three techniques called Diagonal sampling technique, PCA technique and Rechecking technique. They have combined these techniques to improve variable-rate MVQ (CSMVQ). The proposed scheme consists of three phases: preprocessing the received images, encrypting and decrypting. They claim that the proposed scheme is seven times faster than CSMVQ.   [2] proposed a novel picture encryption strategy. The scrambled picture is gotten by arbitrarily changing the stage spectra of the first picture. Subsequently, the subsequent picture is unrecognized and the picture encryption is accomplished.

Manuscript published on 30 December 2019.
* Correspondence Author (s)

Sivaji Satrasupalli, Assistant Professor VFSTR ,Guntur Sivaji.ganesh1100@gmail.com
S Vishnu, Assistant Professor VFSTR ,Guntur.

The stage spectra of the first picture are included with the parallel stage spectra of a pseudo-commotion. This kind of picture encryption is like the private-key cryptographic framework. The study of the attacks for the proposed picture encryption conspire is additionally led. It is demonstrated that the likelihood of a fruitful hacks for a 512 × 512 encoded picture is, probably, 1.25×10^{-11} which requires 84 years by the best in class innovation. The use of this sort of encryption for the dynamic transmission is additionally directed. It is discovered that any piece of the scrambled picture can be utilized to remake an important unique picture. Also, the scrambled picture is uncaring toward the nearness of information misfortune. In this way, in keeping away from the system blockage it is appropriate for the interactive media correspondences. [3] present a picture encryption strategy dependent on PC produced 3D image (CGH) and two-dimensional Sine Logistic regulation guide (2D-SLMM). They consolidate CGH and 2D-SLMM to improve encryption security. Amid the encryption procedure, the 3D image should be strategically adjusted by 2D-SLMM. This calculated tweak procedure can stay away from complex calculations. Reproduction results and security examination show that the proposed methodology has a high security level, great imperceptibility of picture data in ciphertext, substantial key space, and solid heartiness.

[4] present a novel innovation which could stow away advanced picture data dependent on tangram and Conways' diversion. For clarifying the plan, they examined the old tangram confuse and present how to change between two unique pictures. At that point dependent on Conway' diversion, they present a scrambling procedure which conceals the change data. The benefit of this strategy is its security. [5] proposed an encryption technique for pictures. This technique utilizes two technologies to accomplish the compression and encryption. They are the quadtree information structure and the SCAN language, separately. This technique initially compresses the first picture by utilizing a quadtree, and after that encodes the compacted information by SCAN. Along these lines, this technique can compress and encode pictures simultaneously. Quadtree is prominently a lossless information compression technology. Hence, this strategy is additionally lossless.

This work proposes a new encryption strategy to encode and decode the bulk images with less computational time without compromising the security. It comprises of different steps where XOR and shiftings are the basic operations which make the algorithm less weighted and fast.

III. PROPOSED METHOD

In this section, we present the proposed method for the enhanced image encryption and decryption.

3.1 ENCRYPTION:

The following steps are performed in order to encrypt the image.

1. Convert the image into its corresponding bit stream and pad it with zero's if the length of the bit stream is not divisible by 8.
2. Divide the bit stream into two parts of same size and reverse the stream in each individual part.
3. Now, replace left part with right and right part with left.
4. Combine these two parts into one and perform XOR operation with a key of same length as of image bit stream length
5. Divide the obtained result into the parts each of length 8 bits. Collect all left 4 bits into one part and right parts into another.
6. Replace right part of the stream with the result obtained on XORing the left with right and keep left as it is.
7. Perform steps 4, 5 and 6 repeatedly by left shifting the key circularly for every new round.
8. Divide this result into the parts each of length 8 bits. Among those eight bits, leave the left 4 bits as it is and perform circular left shift on the right 4 bits.
9. Combine all these individual parts to generate the cipher text.

3.2 Decryption:

The following steps are performed in order to decrypt the image.

1. Divide the cipher text into the parts each of length 8 bits. Leave the left 4 bits and perform circular right shift operation of right 4 bits.

2. Combine all these 8 bits into one stream.

3. Divide this into two parts. Leave the left part as it is an d replace the right part with XOR of left and right parts.

4. Generate 8 bit parts by collecting left 4 bits from left part and right 4 bits from right part.

5. Combine all these into one stream and perform XOR operation with the key that was used in en cryption.

6. Perform 3, 4 and 5 steps repeatedly by right shift ing the key circularly for every new round.

7. Divide the resultant into 2 parts and replace left part with right and right part with left part.

8. Reverse the bit stream in each part and combine both the parts.

9. Unpad the zero's in the end of the bit stream to get the plain text of original length.

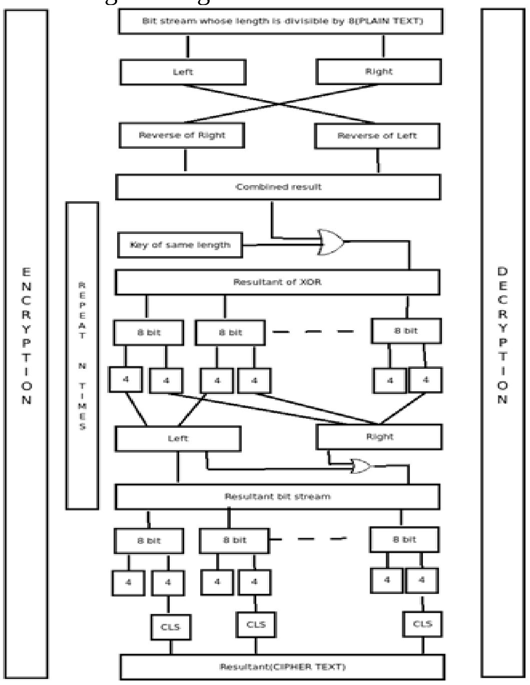

Figure 1: Encryption and Decryption

IV. RESULTS

We have compared the results obtained from the proposed algorithm with that of existing ones in terms of throughput and time taken to encrypt and decrypt the images. Results are shown in below table 1 and it is clear that proposed method outperforms several algorithms such as AES, DES and blowfish in both time and throughput. As shown in below figures, standard images such as nature, medical, space, black and white picture were considered to perform the experiment on.

Figure 2: Nature image

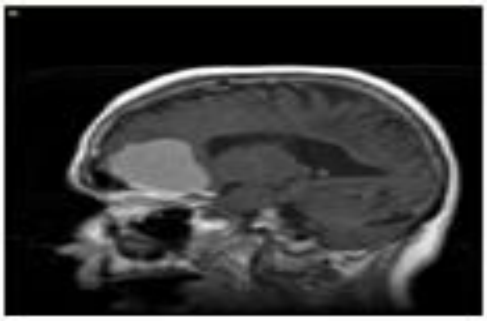

Figure 3: Medical image

Figure 4: Black and white image

Figure 5: Colors image

Figure 6: Satellite image

Table 1: Comparison with existing ones

Image		AES	DES	Blowfish	Proposed
Nature	Throughput	90 KB	48KB	100 KB	**102 KB**
	Encryption	0.076	4.51	0.089	**0.009**
	Decryption	0.0923	5.3279	0.158	**0.014**
Medical	Throughput	101 KB	53 KB	90 KB	**100 KB**
	Encryption	0.0076	3.73	0.07551	**0.0012**
	Decryption	0.0084	4.06	0.08005	**0.0019**
Satellite	Throughput	73 KB	51 KB	93 KB	**105 KB**
	Encryption	0.0035	1.7707	0.0813	**0.00083**
	Decryption	0.0056	2.33	0.096	**0.00096**
Colors	Throughput	86 KB	75 KB	89 KB	**98 KB**
	Encryption	0.008007	4.06	0.0784	**0.0013**
	Decryption	0.0105	4.98	0.0845	**0.0025**
Black and white	Throughput	120 KB	69 KB	82 KB	**91 KB**
	Encryption	0.00255	1.16	0.0905	**0.0009**
	Decryption	0.0047	1.29	0.12	**0.0017**

V. CONCLUSION

This paper presents a symmetric encryption algorithm in which basic operations such as XOR and shiftings are performed in order to encrypt and decrypt images. Though these are the basic operations and if hackers get to know about the key used, it will be very difficult for the hackers to hack the data as it comprises of many intermediate steps and unknown number of XOR operations with the key. In future, we are planning to improve the algorithm by including more number of steps that makes use of less number of operations but hard to decode though key is known.

REFERENCES

1. Chen, T.S. and Chang, C.C., 1997. A new image coding algorithm using variable-rate side-match finite-state vector quantization. IEEE Transactions on Image Processing, 6(8), pp.1185-1187.
2. Kuo, C.J., 1993. Novel image encryption technique and its application in progressive transmission. Journal of Electronic Imaging, 2(4), pp.345-352.
3. Chuang, C.H., Yen, Z.Y., Lin, G.S. and Hong, Z.W., 2011. A Virtual Optical Encryption Software System for Image Security. Journal of Convergence Information Technology, 6(2).
4. Ding, W., Yan, W.Q. and Qi, D.X., 2000. A novel digital image hiding technology based on tangram and Conways' game. In Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101) (Vol. 1, pp. 601-604). IEEE.

5. Chang, H.K. and Liou, J.L., 1994, December. An image encryption scheme based on quadtree compression scheme. In Proceedings of the international computer symposium, Taiwan (pp. 230-237).
6. Diffie, W. and Hellman, M., 1976. New directions in cryptography. IEEE transactions on Information Theory, 22(6), pp.644-654.
7. Chen, T.S. and Chang, C.C., 1997. Diagonal axes method (DAM): a fast search algorithm for vector quantization. IEEE Transactions on Circuits and Systems for Video Technology, 7(3), pp.555-559.
8. Zhao, X.F., 2003. Digital image scrambling based on baker's transformation. Journal of Northwest Normal University (Natural Science), 39(2), pp.26-29.
9. Li, C.G., Han, Z.Z. and Zhang, H.R., 2002. Image encryption techniques: A survey [j]. Journal of Computer Research and Development, 10(023), p.15.
10. Behnia, S., Akhshani, A., Mahmodi, H. and Akhavan, A., 2008. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals, 35(2), pp.408-419.
11. Wong, K.W., Kwok, B.S.H. and Yuen, C.H., 2009. An efficient diffusion approach for chaos-based image encryption. Chaos, Solitons & Fractals, 41(5), pp.2652-2663.
12. Patidar, V., Pareek, N.K. and Sud, K.K., 2009. A new substitution–diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 14(7), pp.3056-3075.