A New Protected Image Transmission Idea via Secret-Splits-Visible Mosaic Images by Nearly Reversible Color Transformations

Pooja Shelar
ME Computer (engineering),
Dr.D.Y.Patil Institute of
Engineering and Technology ,
Pimpri , Pune-411018.
Savitribai Phule
Pune University, India

Archana Chaugule
Department of Computer Engineering,
Dr.D.Y.Patil Institute of
Engineering and Technology ,
Pimpri, Pune-411018.
Savitribai Phule
Pune University, India

ABSTRACT
Secret fragment visible mosaic image is proposed for combining small tiles of secret image to form a target image in the sense of mosaic. When this mosaic image is viewed at close, the observer can view smaller elements, but when viewed at a distance mosaic image is collection of tiles combined together to yield the overall picture. To generate a mosaic image, divide original image into many tiles. Before splitting the image, compare the image for Mosaic creation. Mosaic image is created by composing small tiles of a given secret image in to target image, achieving an effect of embedding the given secret image secretly in the resulting mosaic image. To create the mosaic image, first search a similar target image corresponding to the selected secret image. Then find a best fit secret image tile for embedding in the target image blocks A new secure picture transmission system is proposed, which changes consequently a given expansive volume mystery picture into a purported mystery part noticeable mosaic picture of the same size.

Keywords
Color transformation, data hiding, image encryption, mosaic image, secure image transmission

1. INTRODUCTION
Due to rapid development of computer network technology, it is easy to obtain digital images through network and further use, process, reproduce and distribute them. Digital technology brings us much convenience, but it also gives attacker or illegal user an opportunity. Generally, there are two major approaches which are used to protect digital images.

1.1 Image Encryption
Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation .The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form.

1.2 Information Hiding
One is information hiding which includes watermarking, anonymity, steganography and cover channel. An alternative way to avoid this problem is data hiding. Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. Main drawback of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image.

A new technique for secure image transmission is surveyed, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly lossless from the mosaic image.

The method is in which a new type of computer art image, called secret-fragment-visible mosaic image, is discussed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. But an obvious weakness is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image.

Using previous method, the user is not allowed to select freely his/her favorite image for use as the target image. It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into a secret fragment- visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.

2. LITERATURE SURVEY
J. Fridrich [1] Author demonstrated that several chaos-based image ciphers using a bit-level permutation have been suggested and shown promising results. Due to the diffusion effect introduced in the permutation stage, the workload of the time-consuming diffusion stage is reduced, and hence the performance of the cryptosystem is improved. In this paper, a symmetric chaos based image cipher with a 3D cat map-based spatial bit-level permutation strategy is proposed. Compared with those recently proposed bit-level permutation methods, the diffusion effect of the new method is superior as the bits are shuffled among different bit planes rather than within the same bit-plane. Moreover, the diffusion key stream extracted from hyper chaotic system is related to both the secret key and the plain image, which enhances the security against known/chosen plaintext attack.

G. Chen, Y. Mao, and C. K. Chui [2] **,**Author demonstrated that a variety of effective chaos-based image encryption schemes have been proposed. The typical structure of these

schemes has the permutation and the diffusion stages performed alternatively. The confusion and diffusion effect is solely contributed by the permutation and the diffusion stage, respectively. As a result, more overall rounds than necessary are required to achieve a certain level of security. In this paper, we suggest to introduce certain diffusion effect in the confusion stage by simple sequential add-and-shift operations. The purpose is to reduce the workload of the time consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed.

L. H. Zhang, X. F. Liao, and X. B. Wang [3], First, for the resistance to differential attack and linear attack, they put forward the rather good statistic properties of discrete exponential chaotic maps, In virtue of them, they designed a spatial S-box, and then, then design a key scheme for the resistance to statistic attack and grey code attack. In fact, the scheme can resist to the error function attack (EFA) which be regarded as a very effective attack recently. Finally, Experimental and analytic results show that the scheme is efficient and highly secure.

H. S. Kwok and W. K. S. Tang [4] Another explains picture encryption plan utilizing a mystery key of 144-bits is proposed. In the substitution procedure of the plan, picture is partitioned into squares and in this way into shading segments. Every performing so as to shade part is adjusted bitwise operation which relies on upon mystery key also as a couple of most critical bits of its past and next shading segment. Three rounds are taken to complete substitution process. To make figure more powerful, a criticism component is likewise connected by adjusting utilized mystery key in the wake of scrambling every square. Further, resultant picture is parceled into a few key based element sub-pictures. Every sub-picture goes through the scrambling procedure where pixels of sub-picture are reshuffled inside of itself by utilizing a produced enchantment square lattice. Five rounds are taken for scrambling procedure. The propose plan is basic, quick and delicate to the mystery key. Because of high request of substitution and stage, regular assaults like straight and differential cryptanalysis are infeasible. The exploratory results demonstrate that the proposed encryption strategy is effective and has high security highlight.

S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, [5] Author demonstrated Based on blocked image scrambling encryption; this study presents a new image encryption algorithm by introducing chaos theory. This algorithm firstly makes spatial scrambling based on image blocking in order to interrupt pixel position, then furthering this interruption through Arnold Mapping in the chaos and transforms pixel RGB color space through optimized Arnold Mapping. After this process, we get the final encrypted image through a series of iteration.

J. Tian [6] Author explained a reversible watermarking calculation with high information concealing limit has been created for shading pictures. The calculation permits the watermarking procedure to be switched, which restores the precise unique picture. The calculation shrouds a few bits in the distinction extension of vectors of nearby pixels. The required general reversible number change and the fundamental conditions to maintain a strategic distance from undercurrent and flood are determined for any vector of subjective length. Likewise, the potential payload measure that can be implanted into a host picture is talked about, and an input framework for controlling this size is produced. What's more, to augment the measure of information that can be covered up into a picture, the installing calculation can be connected recursively an over the shading segments. Reproduction results utilizing spatial triplets, spatial quads, cross-shading triplets, and cross-shading quads are given and thought about the current reversible watermarking calculations. These outcomes demonstrate that the spatial quad-based calculation takes into account concealing the biggest payload at the most elevated signal-to-noise ratio (SNR).

V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud [7] Author explained a novel chaos-based pseudorandom permutation–substitution technique for image encryption has been proposed. The pseudorandom number sequences produced through 2D chaotic skew tent map have been used in an effective way to achieve the desired level of confusion and diffusion in the encryption process. All the permutation processes have been made dependent on the plaintext as well as cipher keys, which produce an excellent combination of plaintext sensitivity and key sensitivity in the encryption technique. All the permutation processes have been made dependent on the plaintext as well as cipher keys, which produce an excellent combination of plaintext sensitivity and key sensitivity in the encryption technique.

3. RELATED WORKS

Table.1 Related Works in Secure Image Transmission

Ref no	Paper Title	Technique	Advantages	Result
1	A Symmetric Chaos-Based Image Cipher with an Improved Bit Level Permutation Strategy	Significant diffusion effect is introduced through a 3D cat map-based spatial bit-level shuffling algorithm	It enhances the security against known/chosen plaintext attack	An improved bit-level permutation approach for chaos-based image cipher with permutation diffusion architecture
2	A Fast Image Encryption Scheme based on Chaotic Standard Map	A certain diffusion effect in the permutation stage is introduced by simple sequential add-and-shift operations	Sharing is done effectively.	The effective sharing of the workload in the time-consuming diffusion part is achieved.
3	An image encryption approach based on chaotic maps	A good statistic properties of discrete exponential chaotic maps, In virtue of them, we design a spatial S-box, and then, we design a	The Scheme is efficient and secure	Improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and

		key scheme for the resistance to statistic attack and grey code attack		design a key scheme for the resistance to statistic attack, differential attack and grey code attack
4	Design and analysis of a novel digital image encryption scheme	In the substitution process of the scheme, image is divided into blocks and subsequently into color components	The proposed scheme is simple, fast, and sensitive to secret key	The proposed encryption technique is efficient and has high security features.
5	Analysis and Improvement of Encryption Algorithm Based on Blocked and Chaotic Image Scrambling	This algorithm firstly makes spatial scrambling based on image blocking in order to interrupt pixel position, then furthering this interruption through Arnold Mapping in the chaos and transforms pixel RGB color space through optimized Arnold Mapping	a large key space, high effectiveness and resisting common attack successfully	We get the encrypted image through a series of iteration.
6	Reversible Watermark Using the Difference Expansion of A Generalized Integer Transform	The algorithm allows the watermarking process to be reversed, which restores the exact original image. The algorithm hides several bits in the difference expansion of vectors of adjacent pixels	It has high data hiding capacity	A reversible watermarking algorithm with very high data hiding capacity has been developed for color images
7	A Secure and Efficient Image Encryption Scheme Based on Tent Map and Permutation-substitution Architecture	The pseudorandom number sequences produced through 2D chaotic skew tent map have been used in an effective way to achieve the desired level of confusion and diffusion in the encryption process	A system is robust and completely secured	A novel chaos-based pseudorandom permutation–substitution technique for image encryption has been proposed.

4. CONCLUSION

This paper presents different techniques used for secure image transmission, advantages and disadvantages of existing methods, and also presents a technique which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image . As per survey there is very strong need for secure transmission of secret images in medical and military applications .The goal of this research is to find an advance technique for secure and lossless transmission of secret images

5. REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998

[2] G. Chen , Y. Mao , and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solit. Fract.*, vol. 21, no. 3, pp. 749–761, 2004.

[3] L. H. Zhang , X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solit . Fract.., vol. 24, no. 3, pp. 759–765, 2005.

[4] H. S. Kwok and W. K. S. Tang , "A fast image encryption system based on chaotic maps with finite precision representation," Chaos Solit. Fract., vol. 32, no. 4, pp. 1518–1529, 2007

[5] S. Behnia, A. Akhshani , H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps, "Chaos Solit . Fract., vol. 35, no. 2, pp. 408–419, 2008.

[6] J . Tian , "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890– 896, Aug. 2003.

[7] V. Patidar, N. K. Pareek , G. Purohit, and K. K. Sud , "A robust and secure chaotic standard map base pseudorandom permutation substitution scheme for image encryption," Opt. Commun., vol. 284,no. 19, pp. 4331–4339, 2011.