Grenze International Journal of Engineering and Technology, Special Issue

Implementation of Stegnography on Images using Lossless and Reversible Encryption Methodology

Sravan Kumar Talusani[1], Srikanth Immareddy[2] and Sharmina Bharwani[3]
[1-3]Electronics and Communication Engineering Dept, Methodist College of Engineering and Technology, Hyderabad 500001, India
Email: sravankumartalusani@gmail.com, siri.vlsi@gmail.com, bharwani.sharmin@gmail.com

***Abstract*—The Lossless information concealing gives the embedding of information in a host photo with no loss of information. This study discuss a lossless information hiding as well as photo cryptography technique based upon Chaos Block to picture file encryption the lossless methods if the significant picture is thought about dependable, the embedding distortion could be absolutely gotten rid of from significant photo later the ingrained information has actually been essence. This treatment makes use of attributes of the pixel distinction to install even more information compared to various other arbitrarily dividers making use of Block based Sharpness Index Filtering and also improve with solitary degree wavelet disintegration moving method to avoid photo distortion issues. In this job additionally handles relatively easy to fix information concealing based upon disorderly method. Where originally photo pie chart procedures to regard the pixels which is selected for concealing each little bit of secret information, after that by the logistic disorderly map calculate an order of concealing each little bit stream. Performances separate with various other exist lossless information concealing strategy supplying reveal the supremacy of the study. In this recommended research study PSNR is discovered virtually 5.5 * 103 as well as existing 4.8 * 103 at 100 embedding price which boost for our existing method that substitute in MATLAB 2017a.**

***Index Terms*— chaotic S-block, reversible data hiding, Lossless data hiding, encryption, cryptography, SSI, BSSI.**

I. INTRODUCTION

There are numerous strategies offered for information security. From which security as well as information hiding are 2 reliable ways of information security. The file encryption strategies transform plaintext web content right into unreadable cipher message. The information hiding strategies installed added information right into cover media. The information could be installed by presenting minor adjustments. Information concealing might be carried out with a lossless or relatively easy to fix way. In the suggested system the terms "lossless" and also "relatively easy to fix" will certainly be identified. In the previous referrals these 2 terms have the very same significance.

If the display screen of cover signals consisting of ingrained information is like that of initial cover although the cover information have actually been customized for information embedding, in this situation we could claim that the information hiding technique is lossless. If the initial cover web content could be completely recuperated from the cover variation consisting of ingrained information although a mild distortion has

Grenze ID: 01.GIJET.4.3.37

actually been presented in information installing treatment, in this situation we could state that the information concealing system is relatively easy to fix.

II. Literature Review

Writer Xinpeng Zhang, in his paper" Reversible Data Hiding with Optimal Value Transfer" has actually attempted to enhance the efficiency of relatively easy to fix information hiding. In order to accomplish an excellent payload-distortion efficiency of relatively easy to fix information hiding, his job initially locates the optimum worth transfer matrix by taking full advantage of a target feature of pure haul with a repetitive treatment, and afterwards suggests a sensible relatively easy to fix information concealing plan. The distinctions in between the initial pixel-values as well as the equivalent worths approximated from the next-door neighbors are made use of to lug the haul that is composed of the real secret information to be ingrained as well as the complementary info for initial web content recuperation [5] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, as well as Fenghua Li have actually created the system by scheduling area prior to file encryption. Making the information concealing procedure simple and easy, additional area is made vacant in the previous phase. The approach could make the most of all conventional RDH methods for simple pictures and also attain exceptional efficiency without loss of ideal privacy. Moreover, this unique technique could accomplish genuine reversibility, different information removal and also substantially renovation on the top quality of significant decrypted pictures. Relatively easy to fix information hiding (RDH) in photos is a method, whereby the initial cover could be loss less recuperated after the ingrained message is removed [3] Jessica Fridrich, Miroslav Goljan, Petr Lisonek, and also David Soukal have actually revealed that by utilizing the damp paper coding, one could stand for typically Nd little bits by just turning a component of completely dry aspects where Nd is the variety of completely dry aspects. In this circumstance, the data-hider might turn the completely dry components by changing [6]

III. Proposed Work

A. Lossless Data Hiding Scheme

This scheme involves three parties:
1. An image provider.
2. A data hider.
3. A receiver.

The duty of picture company is to secure each pixel of the initial plaintext photo making use of the general public secret of the receiver. The information hider is not aware with the initial photo. Information hider could change the cipher message pixel worths to install some added information right into the encrypted picture by multi-layer damp paper coding. There exists one problem that the decrypted worths of brand-new as well as initial cipher-text pixel worths should be very same. The receiver have the encrypted photo consisting of the extra information, a receiver understanding the information concealing trick might draw out the ingrained information, while a receiver with the exclusive trick of the cryptosystem could execute decryption to get the initial plaintext photo. The ingrained information could be removed in the encrypted domain name, as well as could not be removed after decryption. That suggests the information embedding does not impact the decryption of the plaintext photo [6]

B. Reversible Data Hiding Scheme

To reduce the photo pie chart some preprocessing is utilized in relatively easy to fix system. After that each pixel is secured with additive homomorphism cryptosystem by the photo company. When information hider has the encrypted photo, he changes the cipher message pixel worths to install a bit-sequence created from the added information as well as error-correction codes. Because of the homomorphism home, the adjustment in encrypted domain name will certainly lead to small increase/decrease on plaintext pixel worth's. The benefit of pie chart diminish prior to file encryption is that the information embedding procedure does not create any kind of overflow/underflow in the straight decrypted picture [7].

C. Combined Data Hiding Scheme

In the lossless system as well as the relatively easy to fix system, the information embedding procedure is executed in the encrypted domain name. The information removal for over 2 systems is extremely various. With the lossless system, information embedding does not influence the plaintext web content as well as information removal is likewise carried out in encrypted domain name. With the relatively easy to fix system,

there is minor distortion in straight decrypted picture could make use of by information embedding, and also information removal and also picture recuperation should be done in plaintext domain name. In the consolidated plan, the picture carrier executes pie chart reduce and also photo security. When having the encrypted picture, the information -hider could install the very first component of added information. On receiver side, the receiver to start with removes the 2nd component of added information from the LSB-planes of encrypted domain name [1].

In both of both systems, the information embedding procedures are carried out in encrypted domain name. On the various other hands, the information removal treatments of both systems are extremely various. With the lossless system, information embedding does not impact the plaintext material as well as information removal is additionally done in encrypted domain name. With the relatively easy to fix system, there is mild distortion in straight decrypted photo brought on by information embedding, and also information removal and also picture healing have to be executed in plaintext domain name. That indicates, on receiver side, the extra information installed by the lossless plan could not be removed after decryption, while the added information installed by the relatively easy to fix plan could not drawn out prior to decryption. In this area, we incorporate the lossless and also relatively easy to fix plans to build a brand-new system, where information removal in either of both domain names is practical. That implies the extra information for numerous objectives might be installed right into an encrypted photo, and also a component of the added information could be removed prior to decryption as well as an additional component could be drawn out after decryption. In the mixed plan, the picture service provider executes pie chart reduce as well as picture file encryption. When having the encrypted picture, the data-hider could install the initial component of extra information utilizing the technique. Signifying the cipher text pixel worths including the very first component of extra information as c'(i, j), the data-hider determines where r''(i, j) are arbitrarily chosen in Z * n or 1 * s+ Z n for Paillier and also Damgard-Jurik cryptosystems, specifically. After that, he could utilize damp paper coding in numerous LSB-planes of cipher text pixel worths to install the 2nd component of added information by changing a component of c'(i, j) with c''(i, j). To puts it simply, the technique is utilized to install the 2nd component of added information. On receiver side, the receiver first of all removes the 2nd component of extra information from the LSB-planes of encrypted domain name. After that, after decryption with his exclusive secret, he removes the initial component of added information as well as recoups the initial plaintext photo from the straight decrypted photo.The illustration of the consolidated plan is displayed in Figure 1. Keep in mind that, because the reversibly ingrained information must be drawn out in the plaintext domain name and also the lossless embedding does not influence the decrypted outcome, the lossless embedding ought to executed after the relatively easy to fix embedding in the mixed system.

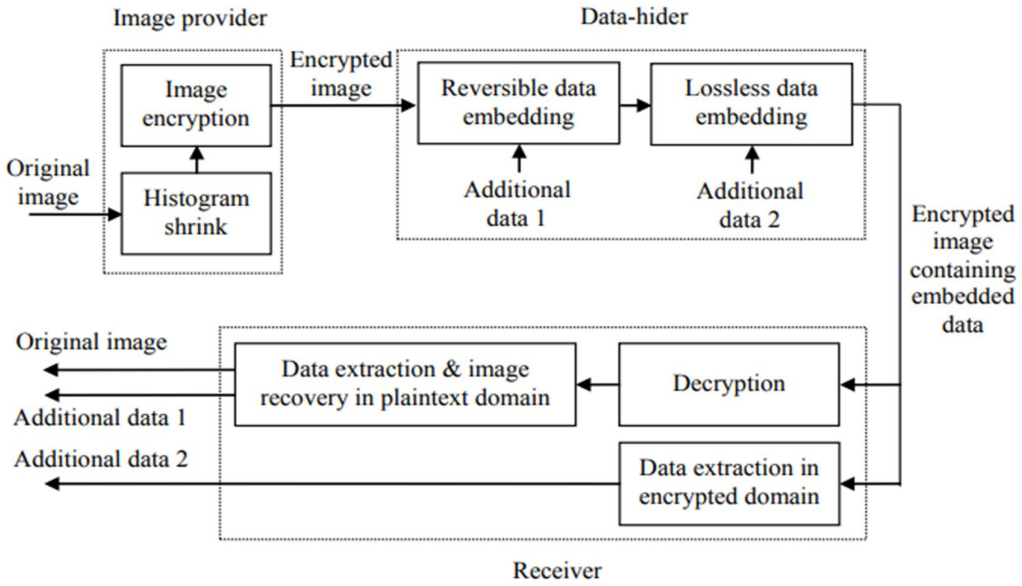

Figure 1. Sketch of combined scheme

IV. Simulation Results

Fig 2 Encryption process

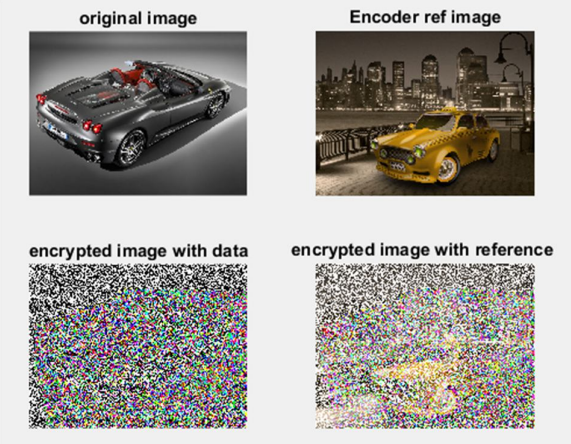

Fig 3 Decryption process

V. Conclusion

In the lossless plan, the ingrained information could be straight removed from the encrypted domain name, as well as the information embedding procedure does not influence the decryption of initial plaintext picture. In the relatively easy to fix system, the extra information could be removed from the plaintext domain name, and also, although a minor distortion is presented in decrypted photo, the initial plaintext photo could be recouped with no mistake. Because of the compatibility of both plans, the information embedding procedures of the lossless and also the relatively easy to fix systems could be concurrently executed in an encrypted picture. So, the receiver could remove a component of ingrained information in the encrypted domain name, and also remove an additional component of ingrained information and also recuperate the initial plaintext picture in the plaintext domain name.

References

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and also Hang Cheng," Lossless and also Reversible Data Hiding in Encrypted Images with Public Key Cryptography",IEEE Transactions on Circuits & Systems for Video Technology.
[2] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish," High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629 − 1636, 2010.
[3] K. Ma, W. Zhang, X. Zhao, N. Yu, and also F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Info Forensics & Security, 8(3), pp. 553-562, 2013.
[4] X. Zhang, "Commutative Reversible Data Hiding and also Encryption," Security and also Communication Networks, 6, pp. 1396 − 1403, 2013. Vol-2 Issue-1 2016 IJARIIE-ISSN(O) -2395 -4396 1578 www.ijariie.com 351
[5] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer, IEEE Trans. On Multimedia, 15(2), 325, 2013
[6] J. Fridrich, M. Goljan, P. Lisonek, and also D. Soukal," Writing on Wet Paper," IEEE Trans. Signal Processing, 53(10), pp. 3923-3935, 2005.
[7] W. Puech, M. Chaumont, as well as O. Strauss," A Reversible Data Hiding Method for Encrypted Images," Security, Forensics, Steganography, as well as Watermarking of Multimedia Contents X, Proc. SPIE, 6819, 2008.
[8] X. Zhang," Separable Reversible Data Hiding in Encrypted Image," IEEE Trans. Details Forensics & Security, 7(2), pp. 526 − 532, 2012.
[9] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316 − 325, 2013.

SRIKANTH IMMAREDDY Received the Bachelor degree in Electronics and Communication Engineering (ECE) from the JNTU Hyderabad India and Master degree in Digital Systems from Osmania University, India in 2009.He is working as Assistant Professor in ECE Dept at Methodist College of Engineering and Technology, India His main interests are in the fields of Very Large Scale Integration and Digital Signal Processing.

SRAVANKUMAR TALUSANI Received the Bachelor degree in Electronics and Communication Engineering (ECE) from Osmania University, India and Master degree in Digital Systems & Computer Electronics from JNTU Ananthapur, India.He is working as Assistant Professor in ECE Dept at Methodist College of Engineering and Technology, India His major interests are in the fields of Analog Electronics and Signal Processing.