Reversible Data Hiding and Image Encryption using Data hiding Algorithm and SVD with Color Partitioning

Priyanka Ugale[1], Prof. S.M.Rokade[2]
[1, 2] Dept of Computer
[1, 2] S.V.I.T Nashik

Abstract- *The framework focuses around Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification. Reversible data hiding (RDH) into encrypted pictures is of expanding regard for analysts as the first content can be perfectly recreated after the installed information are separated while the content owners security stays ensured. The proposed technique receives a color partitioning strategy to utilize the palette color to develop a specific number of embeddable color-triples, whose records are self- embedded into the encoded picture with the goal that an information hider can gather the usable color-triples to embed the secret information. By utilizing the encryption key, the collector can generally recreate the picture content. Analyses have appeared, our proposed strategy has the property that the displayed information extraction and picture recovery are separable and reversible. Our proposed strategy can give a moderately high information embedding payload, keep up high PSNR values of the decrypted and marked pictures, and have a low computational complexity.*

Keywords- Color Partitioning, Encryption, Palette Image, Separable, Data Hiding.

I. INTRODUCTION

Encryption of pictures by utilizing the flipped confirmation with the data hiding key the original picture can encoded and extricated at the recipient side and the content of that owner protection remains secured. The palette picture is utilized as a contribution for the encryption of picture by utilizing the encrypted key. In the picture changes are finished by utilizing the color partition with RGB demonstrate. After the encryption of picture a few information is covered up. For a collector the encoded picture is gotten by utilizing the data hiding key and after that after the picture extracted the original picture is gain.

II. LITERATURE SURVEY

1) Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image".

In this paper, a novel plan for separable reversible data hiding in encrypted image is proposed, which comprises of picture encryption, information embedding and information extraction/picture recovery stages. In the primary stage, the content owner encodes the first uncompressed picture utilizing an encryption key. In spite of the fact that an information hider does not know the original content, he can compress the least huge bits of the encrypted picture utilizing an information hiding key to make an inadequate space to oblige the extra information. With an encrypted picture containing extra information, the beneficiary may extricate the extra information utilizing just the information hiding key, or acquire a picture like the first one utilizing just the encryption key.

2) Wei-Liang Tai and Ya-Fen Chang, "Separable Reversible Data Hiding in Encrypted Signals with Public Key Cryptography"

This paper proposes a different RDH strategy for pictures encoded by public key cryptography. The two ciphertext values are exchanged with one another for embedding the extra information. In view of added content homomorphic properties, we can directly ex- tricate the embedded information from the encrypted domain without knowing the original content. In addi- tion, perfect picture recovery can be straightforwardly handled without earlier information extraction. Since the content protection can be safely safeguarded prepared without earlier information extraction. Since the content protection can be safely saved by Paillier encryption, the proposed plan is proper for cloud administrations without debasing the security level.

3) Dawen Xu, Kai Chen, Rangding Wang, and Shubing Su, “Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification”

In this paper, an algorithm to reversibly embed secret information in encoded pictures is displayed. A particu- lar modulo activity is used to encode the picture, which can save some relationship between the neighboring pix- els. With the saved connection, the information hider can embed the secret information into the encoded picture by utilizing 2D histogram modification, despite the fact that he doesn’t realize the original picture content. Since the embedding procedure is done on encrypted information, our plan protects the secrecy of content. Information extraction is distinguishable from picture decryption; that is, the extra information can be separated either in the encoded area or in the decoded area. Moreover, this algorithm can accomplish genuine reversibility and high caliber of stamped and decoded pictures. One of the conceivable utilizations of this technique is picture annotation in cloud computing where high picture quality and reversibility are greatly desired.

4) M. Hassan Najafi and David J. Lilja, “A High-Capacity Separable Reversible Method For Hiding Multiple Messages In Encrypted Images”

In this paper we proposed a high limit, separable, RDH technique for encrypted pictures which comprises of picture pre-processing, picture encryption, in- formation embedding, and information extraction/picture recreation stages. In the primary stage, the picture is prepared to distinguish the unusual pixels and characterize and embedding frame. The content owner at that point encodes the original picture utilizing an encryption key. One or a few information hiders permute some pre-determined pixels in the embedding frame of the encoded picture utilizing their embedding keys. Every data hider utilizes the MSB of the appointed pixels in the encoded picture to embed a encrypted variant of an extra information stream. In the information embedding stage, the information hider does not really know the original content. At the beneficiary side, with an encrypted picture containing extra information, there will be two unique cases. At the point when the recipient has one or a some of the information embedding keys, the comparing implanted information that are encrypted and hidden inside the encoded picture can be separated. On the off chance that the recipient has the encryption key, the embedded information can’t be extracted without realizing the embedding keys, yet they got information can at present be specifically decoded and the original picture remade with no errors. The recipient does not require the embedding key(s) to recoup the original picture splendidly even with high embedding rates.

III. PROPOSED SYSTEM

The proposed plan is comprised of picture encryption, infor- mation embedding and information extraction/picture recovery stages. The content owner encodes the original uncompressed picture utilizing an encryption key to deliver an encrypted picture. At that point, the information hider packs the least significant bits (LSB) of the encoded picture utilizing an information hiding key to make a meager space to suit the extra information. At the collector side, the information embedded in the made space can be effectively recovered from the encrypted picture containing extra information as indicated by the information hiding key. Since the information embedding just influences the LSB, a decoding with the encryption key can result in a picture like the original version. When utilizing both of the encryption and information covering up keys, the installed extra information can be effectively separated and the first picture can be impeccably recuperated by misusing the spatial connection in characteristic picture.

A. Architecture

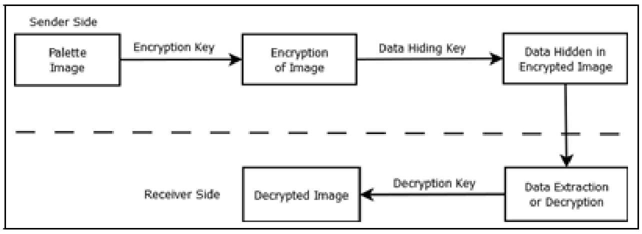


Fig. 1. Proposed System Architecture

B. Algorithms

1) Image Encryption Algorithm:

Step 1: A rectangular matrix A is defined and its transpose AT and AT A product computed.

Step 2: The singular values of A are obtained by computing the eigenvalues of AT A.

Step 3: The diagonal matrix S and its inverse, S−1, are computed.

Step 4: The eigenvectors of AT A are obtained and V and its transpose, V T , computed.

Step 5: U = AV S−1 is computed. The original matrix can be recovered as A = USV T

2) Data Hiding Algorithm:

The basic steps in data hiding algorithm are as follows:

Step 1: Select original image of size M N as input.

Step 2: Message to be hidden is embedded in the RGB pixels of the image.

Step 3: Use pixel selection filter to obtain the best areas to hide the information in the original image to obtain a better rate. The filter is applied to the LSB of every pixel to hide the information, leaving the MSB.

Step 4: After that message is hidden using bit replace- ment method.

Thus secret data is embedded into the image. A.

C. Results

The proposed system is divided into two main parts. First of them is image encryption and second one is data hiding in encrypted image.

Now Image encryption part is completed.

We have calculated value of U, S, V by using following formula,
A = USV T
Where,
A is an m × n matrix
U is an m × n orthogonal matrix S is an n × n diagonal matrix
V is an n × n orthogonal matrix

First user need to provide colored image as a input image and then encrypt that image using SVD (Singular value decomposition algorithm).

Figure 2 shows the input window where user need to provide input image. Figure 3 shows the SVD algorithm process. Figure 4 shows the value of U, V, S. And finally figure 5 shows the final image encryption output. Now in that encrypted image user have to add some text data which will get hide behind that encrypted image.

In this area, we right off the bat dissect our technique regarding the Encryption and Data Hiding. At that point, tests are exhibited to assess the Encryption and Data Hiding. The computational multifaceted nature in down to earth applications is at last talked about. From the substance proprietors perspective, it is requested that the picture substance ought not be gotten by any unapproved recipient. For the information hider, after a color-triple has been installed, the bit-stream of the color-triple ought to be flipped, which results in that, the required XOR estimation of the color-triple will be changed. Since AFC demonstrates the first qualities, all installed color-triples can be recognized by confirming the new XOR values with AFC on the collector side.

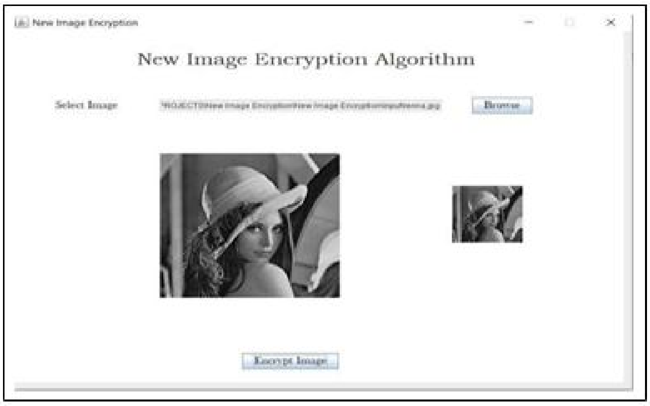


Fig. 2. Selection of Input Image

Fig. 3. SVD Algorithm

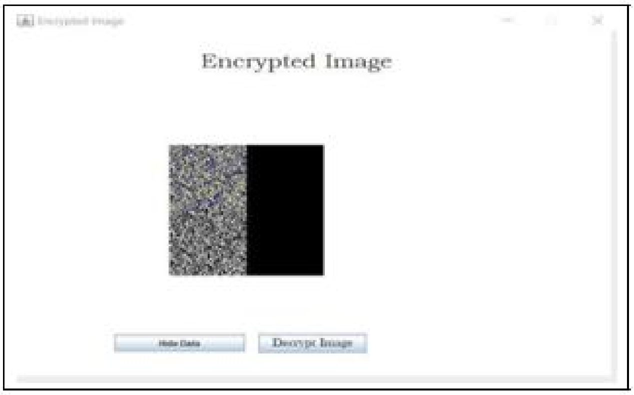


Fig. 4. Encrypted Image

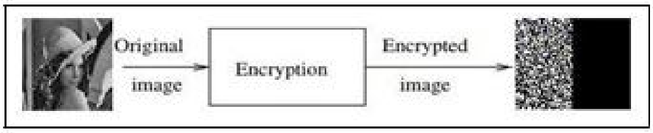
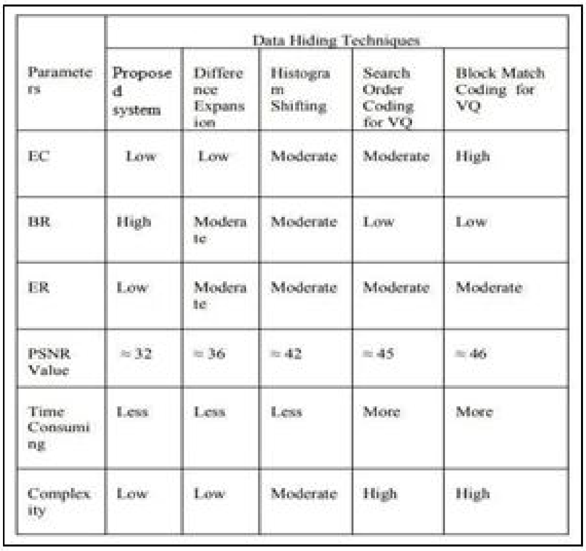


Fig. 5. Final Image Encryption Output

D. Performance Comparison



Parameters	Data Hiding Techniques				
	Proposed system	Difference Expansion	Histogram Shifting	Search Order Coding for VQ	Block Match Coding for VQ
EC	Low	Low	Moderate	Moderate	High
BR	High	Moderate	Moderate	Low	Low
ER	Low	Moderate	Moderate	Moderate	Moderate
PSNR Value	≈ 32	≈ 36	≈ 42	≈ 45	≈ 46
Time Consuming	Less	Less	Less	More	More
Complexity	Low	Low	Moderate	High	High

Fig. 6. Performance Comparison Table

Data hiding techniques is getting popular due of the importance in securing secret data from unauthorized users or attackers. In this paper five different types of data hiding techniques for digital images: Proposed system technique, Difference expansion technique, Histogram modification technique, Search order coding technique and Block match coding technique are studied, analyzed and compared. Parameters like embedding capacity, bit rate, embedding rate etc are used

to compare the performance of different techniques. Most of the techniques discussed are reversible. Reversible data hiding techniques achieves real reversibility that is the cover image can be extracted completely at the decoder.

E. System Requirements Software Requirement:

- Operating System : Microsoft Windows 7 or Above
- IDE : Netbeans 8.2
- Language : Java 1.8
- Databese : MySql 5.5

Hardware Requirement:

- Processor : Core Intel 3 or Above
- RAM : 2 GB or Higher
- Hard Disk : 50 GB (min)

IV. CONCLUSION

In this paper, a novel plan for separable reversible data hiding in encrypted image is proposed, which comprises of picture encryption, information embedding and information extraction/picture recovery stages. In the primary stage, the content owner encodes the first uncompressed picture utilizing an encryption key. In spite of the fact that an information hider does not know the original content, he can compress the least huge bits of the encrypted picture utilizing an information hiding key to make an inadequate space to oblige the extra information. With an encrypted picture containing extra information, the beneficiary may extricate the extra information utilizing just the information hiding key, or acquire a picture like the first one utilizing just the encryption key. At the point when the beneficiary has both of the keys, he can extricate the extra information and recover the original content with no error by misusing the spatial connection in normal picture if the measure of extra information isn't excessively substantial.opted Images".

REFERENCES

[1] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image".IEEE Transactions On Information Forensics And Security, Vol.7, No. 2, April 2012.

[2] Wei-Liang Tai and Ya-Fen Chang, "Separable Reversible Data Hiding in Encrypted Signals with Public Key Cryptography" www.mdpi.com/journal/symmetry, 2018.

[3] Dawen Xu, Kai Chen, Rangding Wang, and Shubing Su, "Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification", Security and Communication Networks Volume,2018.

[4] M. Hassan Najafi and David J. Lilja, "A High-Capacity Separable Reversible Method For Hiding Multiple Messages In Encrypted Images".