INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Secure Data Hiding in Images within Selected Zones

Neha Manjrekar
K.J. Somaiya College of Engineering, VidyaVihar, Mumbai, India
Shruti Savant
K.J. Somaiya College of Engineering, VidyaVihar, Mumbai, India
Deepashri Chavan
K.J. Somaiya College of Engineering, VidyaVihar, Mumbai, India
Heena Azmi
K.J. Somaiya College of Engineering, VidyaVihar, Mumbai, India
Grishma Sharma
Professor, Computer Department
K.J. Somaiya College of Engineering, VidyaVihar, Mumbai, India

Abstract:
Security has become one of the most significant problems in distributing new information. It is necessary to protect this information while communication over insecure networks. Cryptography and Steganography[7][8] are two major techniques for secret communication. This paper presents a high security model by combining cryptography and steganography[7][8] techniques which encrypts the text data and then hides the encrypted data in the robust regions of the image. It will facilitate secret communication through images without letting the third party get aware of the secret communication. This will take place in the cover media which will be an image. The data to be transmitted will be encrypted using AES[3][6] and whirlpool[9][10], the robust regions in the cover media will be extracted using SURF[1][11][12], the encrypted data will be embedded using LSB[2][13][14] in these obtained regions and then the stego image will be produced. The key for encryption and decryption has to be same. Thus the system is implemented and the data remains hidden from the intruder or eves-dropper.

Key words: *AES, Whirlpool, SURF, LSB matching*

1. Introduction

Privacy and secrecy is a concern for most people during information exchange via any medium. Data hiding is nothing but hidden communication. It deals with concealing the existence of the message. It is related to cryptography and steganography [7][8] whose intent is to render messages unreadable except by the intended recipients. Data hiding within cover improves the data security of critical data that is to be transmitted, thus allowing the parties to communicate secretly and covertly.

The drawbacks of previous systems were that they were not robust and were easy to decrypt.

The proposed framework overcomes these drawbacks. The flow of the system is as follows:

- Applying multilevel encryption using whirlpool [9][10] and AES. Our input key will be encrypted by whirlpool [9][10] and then used as a key for AES. The data is then encrypted by AES.
- The input image is taken and SURF [1][11][12] is applied to get the robust regions.
- The encrypted data is then embedded in the robust regions of the image using LSB [2][13][14]. Thus stego image is generated which will be transmitted.

The stego image will hold the secret information and renders it invisible to the other users who are not aware of the secret communication.

This paper is organized as follows: Section II discusses the proposed framework which includes detail description of the modules in section a, b, c, and d. Section III presents the workflow the system and finally we conclude this work in Section 4.

2. Proposed Framework

2.1. AES

The AES algorithm is a symmetric key bock cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used to both encrypt and decrypt a message. Also, the cipher text produced by the AES algorithm is the same size as the plain text message. Most of the operations in the AES algorithm take place on bytes of data or on words of data 4 bytes long, which are represented in the field GF (28), called the Galois Field. AES is based on a design principle known as a Substitution permutation network. AES operates on a 4*4 matrix of bytes, termed the state. The AES cipher is specified as a number of repetitions of transformations rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. AES is fast in both software and hardware.

High-level description of the algorithm

The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

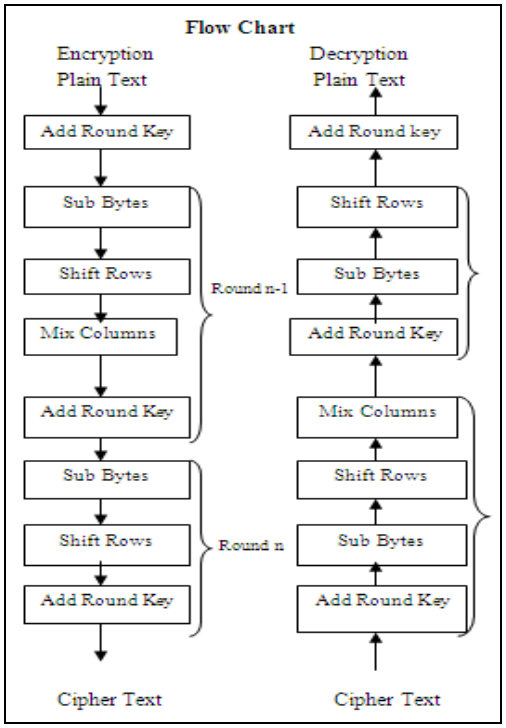

Figure 1

- Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
- Initial Round
  Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
- Rounds
  Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
  Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
  Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  Add Round Key
- Final Round (no Mix Columns)
  Sub Bytes
  Shift Rows
  Add Round Key.

2.2. Whirlpool

Whirlpool [9][10] is a Cryptographic hash function using block cipher. It works by taking the original message, anything shorter than 2^{256} bytes, hashing scheme, and a block cipher to produce a 512-bit message digest, or hash value, for the input message. The following diagram depicts work of a whirlpool [9][10] Message Digest.

whirlpool[9][10] came from the fact that even a small change to the original message will produce a vastly different message digest, to the point that they will appear completely unrelated, making it very strong algorithm. The common uses of whirlpool [9][10] are password verification, file verification, and digital signing.

Sub Bytes: The Sub Bytes operation applies a non-linear permutation (the S-box) to each byte of the state independently. The 8-bit S-box is composed of 3 smaller 4-bit S-boxes.

Shift Columns: The Shift Columns operation cyclically shifts each byte in each column of the state. Column *j* has its bytes shifted downwards by *j* positions.

Mix Rows: The Mix Rows operation is a right-multiplication of each row by an 8×8 matrix over $\mathbb{F}_{2^8}$. The matrix is chosen such that the branch number (an important property when looking at resistance to differential cryptanalysis) is 9, which is maximal.

Add Round Key: The Add Round Key operation uses bitwise xor to add a key calculated by the key schedule to the current state. The key schedule is identical to the encryption itself, except the Add Round Key function is replaced by an Add Round Constant function that adds a predetermined constant in each round.

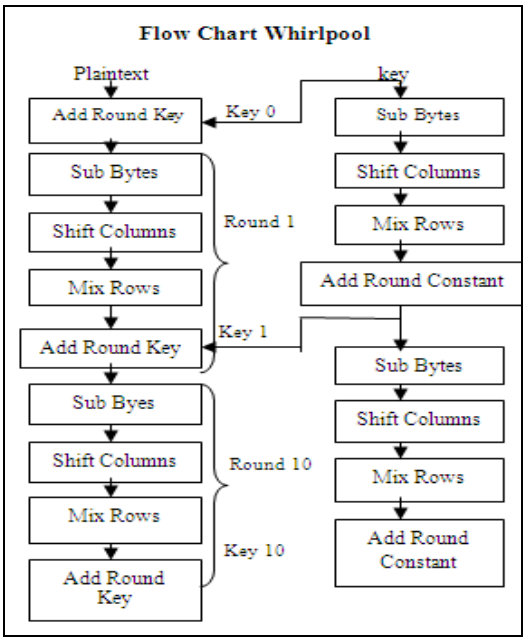

Figure 2

2.3. Selecting of the Zones in the Cover Media for Embedding

The modified embedding of the cipher text will be applied in selected areas of the image only. These selected areas will be the robust interest points in the image. Thus increasing the invisibility of the cipher text being present in the cover object. This will be implemented using a technique called "SURF [1][11][12]", speeded up robust feature.

The SURF [1][11][12] techniques is favored in the present work, because of its robustness and high speed that is several times higher than the SIFT. SURF [1][11][12] has been known, to tackle the problem of point and line segment correspondences between two images of the same scene or object. The latter in turn can be part of many computer vision applications. The SURF[1][11][12] approach can be divided into three main steps. First, key-points are selected at distinctive locations in the image, such as corners, blobs, and T-junctions. Next, the neighborhood of every key-point is represented by a feature vector. This descriptor has to be distinctive. At the same time, it should be robust to noise, detection errors, and geometric and photometric deformations. Finally, the descriptor vectors are matched among the different images. Key-points are found by using a so called Fast-Hessian Detector that is based on the approximation of the Hessian matrix for a given image point. The responses to Haar wavelets are used for orientation assignment before the key-point descriptor is formed from the wavelet responses in a certain surrounding to the key-point. Therefore, the SURF [1][11][12] constructs a circular region around the detected key-points. Second, the SURF[1][11][12] descriptors are constructed by extracting square regions around the key-points. Such a process results in a descriptor of sixty four-length. Fig. 3 shows an example of the detected key-points using the Fast-Hessian detector. Accordingly, the SURF [1][11][12] is exploited in this paper to calculate the invariant key-points in the cover image. The key-points will be the centers of the regions in which the information is to be embedded. Depending on the size of the required regions, some points will not be used to avoid any intersections,

resulted from the very close key-points. To guarantee that the local regions are disjoint, each point should be considered by calculating the Euclidian distance d. The calculation of the latter should be between the selected points and among all other points in the list.

All d values should be greater than 2 2r as the size of the embedding region is 2r ∗ 2r as shown in Fig. 4.

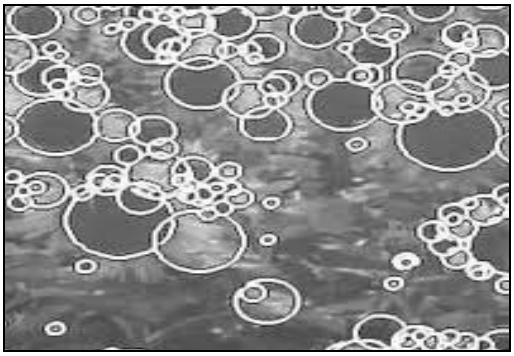

Figure 3: Example of detected interest points for a Sunflower field using SURF [1][11][12]

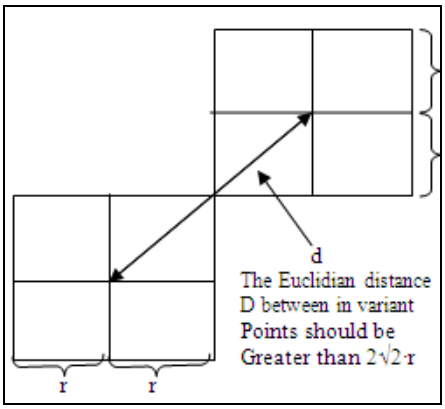

Figure 4: Examining regions to avoid intersections

2.4. Embedding the Encrypted Cipher Text into the Zones of the Cover Media

After the message has been encrypted and the zones from the image detected, the message will be embedded in these found out zones. Block diagram for SURF [1][11][12]:

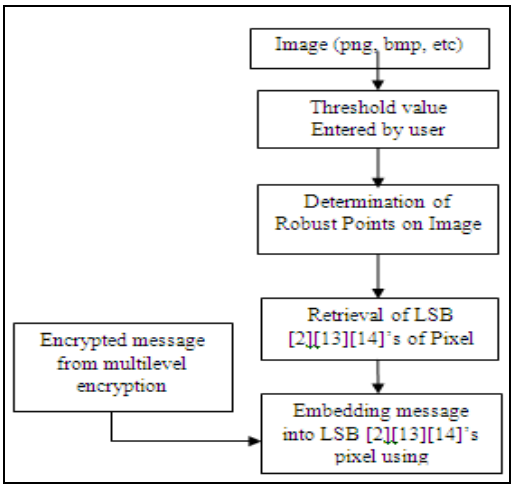

Figure 5

This will be done by the LSB [2][13][14] algorithm.

"Least Significant Bit algorithm"

(LSB[2][13][14]) by which the least significant bits of the secret document are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. The LSB [2][13][14] encoder replaces the least significant bit of pixel values with the encrypted information bits. The modified picture is now termed as Stego image.

Thus, we have modified the LSB [2][13][14] algorithm to embed the secret text into the host image.

3. Work Flow

We are developing a system in which we are performing multilevel encryption. The following flowchart depicts the data flow of the systems at the sender's side.

- In encryption, the input message will undergo multi-level cryptography technique. Initially we select secret message using AES algorithm by using key that is provided by user. These encryption key first hash with whirlpool [9][10] hash function and apply AES encryption on secret message.
- The modified cipher text will be applied in selected areas of the image only. These selected areas will be the robust interest points in the image. This will be implemented using a technique called "SURF [1][11][12]", Speeded Up Robust Feature.
- The message has be been encrypted and the zones from the image are detected, now the message will be embedded in these found out zones. This will be done by LSB[2][13][14] technique, subsequently the LSB[2][13][14]'s of the pixel of host image interest points will be retrieved and the individual bit of encrypted message stream will be embedded into those LSB[2][13][14]'s .
- The secret message has been embedded, to increase its invisibility and the probability of being detected easily is decreased, by performing a refinement in the cover image (stego-image).
- The neighboring pixels of those selected interest points of the image where the embedding has been done will be modified according to the concerned point.

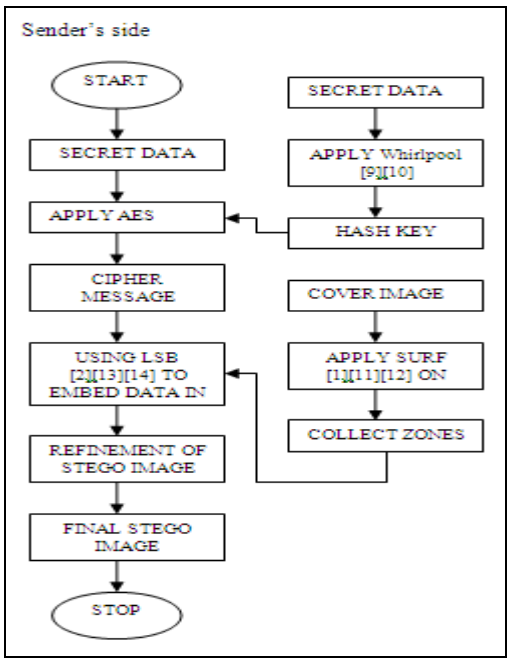

Figure 6

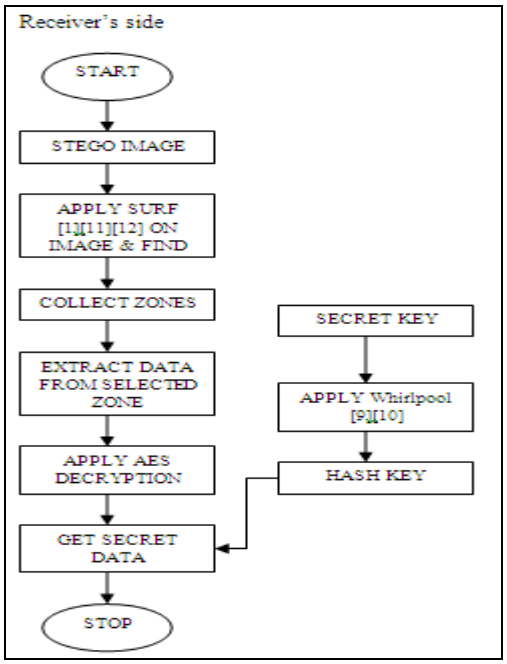

Figure 7

The following flowchart depicts the data flow of the system at the receiver's end. Here the steps will be performed in the reverse manner. This extraction of the hidden data from the cover media is called as Steganalysis. Here we will apply it for extracting the hidden data. This will be done in the following manner as presented in the flowchart.

4. Conclusion

In this paper, a novel data hiding scheme based on SURF [1][11][12] is proposed. Detailed experiment has been carried out and it is found that our proposed algorithm is able to embed text strings into the color host image. The proposal is initiated by a password supplied by the user. With the proposed application, text passing in hidden form through digital color image is done in a very efficient manner. In the encrypted image the embedded text is entirely invisible. The whole embedding process consists of two parts. The first is encrypting the text string with multi level encryption using whirlpool [9][10] and AES algorithm. The second is data/ secret bits embedding into the cover image are only embedded in the robust zones selected by SURF [1][11][12] technique. The text extraction framework is blind that guarantees, except the secret key nothing is needed to extract the hidden text from encrypted image. The 32-bit secret key and an efficient whirlpool [9][10] hash function with AES encryption ensure high security aspects. Moreover the implemented application software is extremely user friendly

Here the data hiding is achieved using the characteristic regions of the image while secret binary data is embedded in them. These robust characteristic regions are relatively limited. The parameters like robustness and payload capacity are at odd with each other. So attempts to encrypt larger data might slow down the system, so it will sacrifice the computation time.

For future work, we expect to enhance the proposed scheme. This may be achieved by adopting different data hiding techniques to embed the data.

5. References

1. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah Al-Qershi, "Characteristic Region Based Image SteganographyUsing Speeded –Up Robust Features Technique", Communication and Computer Engineering School University Malaysia Perlis(UniMap) Perlis, Malaysia
2. Soumik Das, Pradosh Bandyopadhyaya, Prof. Atal Chaudhari , Dr. Monalisa Banerjee, "A Secured Key-Based Digital Text Passing system Through Color Image Pixels", MCA dept, techno India, Salt Lake, India.
3. Edward Roback and Morris Dworkin (NIST),"FIRST ADVANCED ENCRYPTION STANDARD (AES) CANDIDATE CONFERENCE", Ventura ,CA August 20-22, 1998(U.S. Government work not protected by U.S. copyright.)
4. Davey Alba,"Scrambled Code Keeps Software Safe", A new form of encryption could make practically unhackable code,Posted 26 Sep 2013
5. 1619.2-2010 - IEEE Standard for Wide-Block encryption for Shared Storage Media
6. Joan Daemen, STMicroelectronics Vincent Rijmen, Katholieke Universities Leuven, "The First 10 Years of Advanced encryption" November/December 2010 (vol. 8 no. 6)pp. 72-74 DOI Bookmark http://doi.ieeecomputersociety.org/10.1109/MSP.2010.193
7. H. B. Karaman, S. Sagiroglu, Comput. Eng. Dept., Gazi Univ. Eng., Ankara, Turkey "An Application Based on Steganography" Istanbul Turkey August 26-August 29 DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/ASONAM.2012.152
8. Ali A. Al-Ataby,Fawzi M. Al-Naima, "High Capacity Image Steganography Based on Curvelet Transform" Dubai, United Arab Emirates December 06-December 08 ISBN: 978-0-7695-4593-6
9. Peter Gutmann, University of Auckland David Naccache, Gemplus Charles C. Palmer, IBM, "When Hashes Collide" May/June 2005 (vol. 3 no. 3)pp. 68-71 DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/MSP.2005.84
10. Ricardo Chaves , Georgi Kuzmanov, Leonel Sousa, "Merged Computation for whirlpool Hashing",Munich, Germany March 10-March 14 ISBN: 978-3-9810801-3-1 DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/DATE.2008.4484896
11. Yong-Hwan Lee,Yukong Lee,Hyochang Ahn, Je-HoPark, Youngseop Kim, " Implementation of Image Descriptor Based on SURF and DCD",Suwon, Korea (South), June 24-June 26,ISBN: 978-1-4799-0602-4
12. Nabeel Younus Khan, Brendan McCane, Geoff Wyvill, "SIFT and SURF Performance Evaluation against Various Image Deformations" , on Benchmark Dataset Noosa, Queensland Australia December 06-December 08 ISBN: 978-0-7695-4588-2
13. Guangjie Liu, Zhan Zhang, Yuewei Dai, Zhiquan Wang, "GA-Based LSB-Matching Steganography to Hold Second-Order Statistics" Hubei, China November 18-November 20 ISBN: 978-0-7695-3843-3,DOI Bookmark http://doi.ieeecomputersociety.org/10.1109/MINES.2009.281
14. Chin-Chen Chang, Hsien-Wen Tseng, " Data Hiding in Images by Hybrid LSB Substitution" Qingdao, China June 04-June 06 ISBN: 978-0-7695-3658-3,DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/MUE.2009.68