# Bit-Plane Slicing Algorithm for Crime Data Security using Fusion Technologies

**Shaik Akbar, K.Nageswara Rao, T.Anand**

***Abstract: Security in today's world has become a critical issue. Information should be made very secure providing access only to authorized persons. Unaccredited persons should not be given access to the data. Cyber Department is the one which in search of the innovative ideas in order to secure this crime data. Forensic Science that is an application of science plays a vital role in undertaking the investigation of crimes and criminal justice using some scientific methodologies. Also, Steganography is the skill with which the data can be hidden or protected within another data (i.e data inside data with security). This paper brings out the integration of both Forensic Science and Steganography that gives rise to a hybrid technology for securing the crime data. The concept of Data embedding strengthens the Steganography method. The most appropriate method adapted in this paper is the use of finger prints of the crime persons. These gathered finger prints are divided into eight slices by using the "Bit plane slicing" algorithm. Any official data that is in reference with the crime data is being kept in any one of these eight slices. The main theme of this proposed paper is to secure the crime data in these finger prints.***

***Key Words: Cyber Department, Steganography, Forensic Science, Data Embedding,Finger Prints, Bit-plane slicing algorithm.***

## I. INTRODUCTION

Cryptography is the most frequently used technique where the data is being encrypted to ensure security from the eavesdroppers. But this method does not totally ensure the data security. For this, here we are implementing Steganography rather than cryptography. Steganography is the technique which is an "invisible" communication where the data is being maintained very secured by embedding all the crime related data in a photo which is in the form of finger print picture. The finger print picture will contain all the official and confidential data with high security and uses encryption and decryption techniques to access the data. This process of data security involves two main steps:

- Embedding the data
- Extracting the data

Every Steganography process objective is to maintain minimal amount of time in executing the data embedding and data extraction with lowest probability of encountering errors. The use of steganography does not change the original finger print image. It just embeds the secret data in the picture which resembles same as the original picture. This paper entails the bit slicing algorithm in order to embed the secret data in any slice of the eight slices. In this technique each pixel is represented by 8 bits. The whole image consists of 8 -bit plane. Plane- 0 consists the LSB (Least Significant Bit) and the Plane-7 consists the MSB(Most Significant Bit).

The partition of the digital picture into bit planes is helpful in determining the importance and role of each bit of image. It also specifies the total number of bits needed to quantize each pixel which is also useful for image compression.

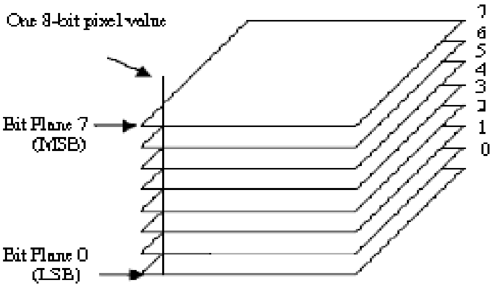


**Fig 1: Bit-Plane Slicing**

The number of bit-planes used to partition the image is directly proportional to the security level. Encryption of the MSB bit is most recommended method because the picture degradation is less. If we choose the encryption for LSB bit, then the chance of image degradation is more than the MSB bit encryption. In order to avoid this degradation, the encryption should be done carefully in any of the plane without changing the original image. In order to strengthen the encryption process, the image encryption is to be made more difficult by rotating the bit-plane at different angles.

## II. TYPES OF STEGANOGRAPHY

Steganography can be categorized into the following types based on the cover medium they use.Cover medium can be any of the type: text, image, audio or video file. The various types of Steganography are:

i) Text Steganography
ii) Image Steganography
iii) Audio / Video Steganography

## III. IMPLEMENTATION

Assume a finger print image which is composed of a number of pixels where each pixel is represented in terms of bits. And bit plane is composed of 8 bit planes in which the LSB has the lower order bits of pixel and MSB has higher order bits of pixel of an image. Bit plane rotation technique is used for encryption of crime data.

**Revised Manuscript Received on December 08, 2018.**

**Dr. Shaik Akbar,** Professor, Dept.of CSE, PSCMR College of Engineering and Technology, Vijayawada, AP, India

**Dr.K. Nageswara Rao,** Principal, PSCMR College of Engineering and Technology, Vijayawada, AP, India

**T. Anand,** Associate Professor, Dept.of CSE, PSCMR College of Engineering and Technology, Vijayawada, AP, India

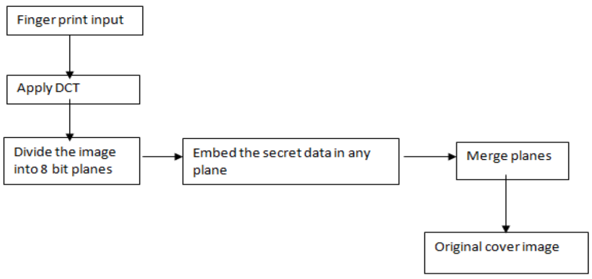

Finger print input
Apply DCT
Divide the image into 8 bit planes
Embed the secret data in any plane
Merge planes
Original cover image

**Figure 2: Proposed Model**

The secret message is encrypted and integrated in any one of the bit planes only after rotating the bit plane image into various angles such that the eavesdroppers cannot understand which technique is used in encryption .Here, encryption and decryption process of the crime data is based on the bit plane slicing. The sample input finger print image is as indicated below:

**Figure 3: Sample input image**

Every input finger print image is first divided into eight slices by using bit-plane slicing algorithm and then each pixel of plane is rotated at various angles. The rotation process of plane does not result in any bit loss or disturb the original image.

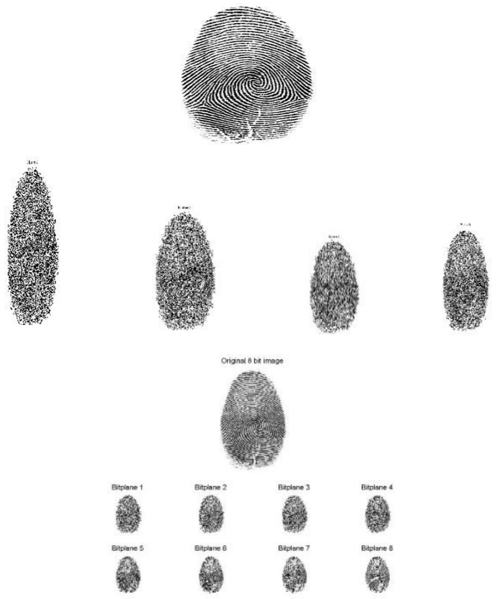


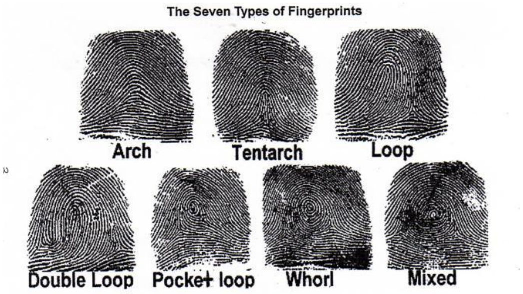
**Figure 4: Bit Slice of an original image**

The confidential data is encrypted and embedded in any one of the slices in different angle of the image. At the end all the eight planes are integrated to form the original cover image. This kind of encryption technique involves the decryption without any information loss.

Bit slicing followed by concealing the information is more efficient in grey scale image than compared to a coloured image.

Finger prints can be categorised into seven types as following:

- Arch
- Tetrarch
- Loop
- Double Loop
- Pocked Loop
- Whorl
- Mixed



Arch- the arched lines are like waves going from one site to the other site.

Tentarch- like the Arch but with a rising stick in the middle.

Loop- the lines coming from one site returning in the middle to the same side.

Double Loop- like the Loop but with two loops inside, one standling, one hanging.

Pocke+ Loop- like the loop but with a small circle in the turning point.

Whorl-the lines are making circles.

Mixed Figure- composed with different figures.

**Figure 5: Different types of Fingerprints**

Data that embedded in the compressed image of finger print provides more security. A comparative analysis is made in three ways,

i. Embedding the data in the original image.
ii. Embedding the data in different bit planes.
iii. Embedding the data after compressing the bit planes.

*Algorithm:*

Step 1: Get finger print as input.
Step 2: Divide the finger print into eight bit plane.
Step 3: Rotate each bit plane in multiple angles.
Step 4: Conceal the confidential data in any one of the bit-plane.
Step 5: Merge the planes
Step 6: Original cover image and also the data embedded image must be matched.

## IV. RESULTS

*PSNR:*

Peak Signal Noise Ratio (PSNR) is the unit of measurement between the cover image and the encrypted image. If this PSNR value is less then it indicates the cover image and the encrypted image are not same.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

$$\mathrm{PSNR} = 10\log_{10} \times \frac{\mathrm{Maximum}}{\mathrm{MSE}}$$

*MSE:*

Mean Square Error (MSE) is indirectly proportional to PSNR. In this a comparison is made between the original and half of the embedded image.

| **Type of Finger print** | **PSNR** | | |
|---|---|---|---|
| | **Original image** | **Bit plane image** | **Compressed image** |
| **Arch** | 70.5 | 78.0 | 80.1 |
| **Loop** | 61 | 67.1 | 72 |
| **Whorl** | 80 | 84.0 | 88.5 |

| **Type of Finger print** | **MSE** | | |
|---|---|---|---|
| | **Original image** | **Bit plane image** | **Compressed image** |
| **Arch** | 32 | 28 | 21.6 |
| **Loop** | 33 | 28 | 26.1 |
| **Whorl** | 25.2 | 22 | 18.1 |

The outcome of this paper is measured by the values of PSNR and MSE. The implementation of Bit plane slicing algorithm is found to be very effective as no data loss occurs in encryption and decryption. The image quality and security purely depends on the bit plane slicing. Hence, the proposed paper provides the security to greatest level.

## V. CONCLUSION

This paper chooses bit plane slicing technique with which the data can be made more secured and cannot be hacked easily by eavesdroppers. The merging of planes is done by comparing the adjacent bits of the image. All the crime related data is maintained in this finger print image only. Not only securing the image is considered, but also the quality of image is required.

## REFERENCES

1. Andreas Westfeld and Andreas Pfitzmann. Attacks on Steganographic Systems 1999. In Proceedings of Information Hiding - Third International Workshop. Springer Verlag, September 1999.
2. Evaluation of various LSB based methods of image Steganography on GIF file format – Namita Tiwari, International Journal of Computer Applications, September 2010.
3. “Security for an Image using Bit-slice Rotation Method-image Encryption” by R.Vijayaraghavan, S.Sathya and N.R.Raajan.
4. Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998.
5. Lee Yeuan-kuen et al, “An Advanced Least-Significant- Bit Embedding Scheme for Steganographic Encoding”, 5414/2009: pp. 349-360, 2009.
6. Johnson, N.F. Jajodia, S.& Duric, Z., 2001. Information hiding: steganography and watermarking – attacks and countermeasures. Kluwer academic publishers.
7. Li Zhi,Sui Ai Fen, “Detection of Random LSB Image Steganography”IEEE pp2113-2117,2004.
8. J. R. Smith and B. O. Comisky, “Modulation and information hiding in images,” in Information Hiding, First International *Workshop,* Lectu e Notesin Computer Science, R. Anderson, Ed. Berlin, Germany:Springer-Verlag, 1996, vol. 1174, pp. 207–226.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*