Real Time MMS Security For Mobile Communication Using Steganography

Chinar Bhandari [#1], Ashish Bandi[#2], Sonu Gupta[#3] , Avinash Jadhav[#4]

[#]*Computer Department, University Of Pune*
AISSMS's IOIT, Kennedy Road, Shivajinagar, Pune-411001, Maharashtra, India.
[1]chinarbhandari@gmail.com, [2]ashishbandi123@gmail.com
[3]sonugupta4636@gmail.com, [4]avinashjadhav1993@gmail.com

Abstract— **The Multimedia Messaging System allows a user of a mobile phone to send messages containing multimedia objects, such as images, audio or video clips. MMS has very quickly gained the popularity of SMS among mobile users. Alongside, the need for a secure communication became more imperative. Hiding information, especially in images has been an attractive solution for secret communication. In this paper we examine the possibilities for the use of steganography within a multimedia message. The most widely known algorithms for steganography like BPCS are presented and discussed. Their application in a mobile environment is analyzed and a theoretical evaluation is given.**

Keywords— **Steganography, data hiding, information hiding, BPCS, digital picture envelope, stego-key, vessel image, dummy image, encryption, Decryption, bit plane.**

.

I. INTRODUCTION

One of the most popular uses of mobile phones has been the exchange of messages between users. [2]The Short Messaging System (SMS) was introduced with GSM mobile phones and it very rapidly became popular among users. The Multimedia Messaging System (MMS) offers the ability to send and receive multimedia content using mobile phone. Nowadays, most of the mobile phones not only are capable of sending and receiving Multimedia Messages (MM), but also contain an embedded camera and can run customized applications.

Most research regarding security in mobile environments with limited resources in terms of processing power, memory capacity and energy autonomy, is focused on the implementation of symmetric and asymmetric cryptographic algorithms. Steganography differs from cryptography in the sense that it tries to hide the message instead of transforming it so as to obscure its meaning. In some cases, steganography may actually prove to be more effective. The combination of both may give the best results, as a message can be encrypted before it is hidden into another object. [1]Cryptography has received most attention until now, leaving a great space for research on steganography. Steganography concerns itself with ways of embedding a secret message into a cover object, without altering the properties of the cover object evidently. The embedding procedure is typically related with a key, usually called stego-key.Without knowledge of this key it will be difficult for a third party to extract the message or even detect its existence. Once the cover object has data embedded in it, it is called a stego object. The amount of data that can be hidden in a cover object is often referred to as embedding capacity. The embedding capacity is directly relatedwithc the secrecy of the message. The distortions in the cover object caused by the steganographic algorithm become more obvious as a user tries to add more hidden data. Evidently, there is a point of balance when the embedded data do not alter the cover object significantly enough to arouse suspicion.

In this paper we examine how steganography can be used in the context of MMS. To the best of our knowledge, there are only very few known implementations of Steganographic algorithms for mobile devices. We present some widely used algorithms for Steganographic and explain how they can be applied in MMS. Users can benefit from covert channels in MMS in order to secretly exchange hidden messages and keys, without affecting suspicion of their existence. It could also be used as a mean for hiding the exchange of one-time passwords between a corporate server and a mobile worker. An evaluation of Steganographic techniques is also required, as, to the best of our knowledge, there has not been any benchmarking of steganographic algorithms. We propose assessment metrics that can provide us with a sufficient view of their performance. The structure of this paper is as follows: Initially, we present the Steganographic algorithms that can be used in the MMS. These algorithms can be applied to image, audio or video files, but also can be applied for information presentation and we also explain embedding capacity for each image. In following section we present Steganographic techniques are evaluated and some examples of their applications are given. Finally, we provide our concluding remarks and give suggestions for future research [3] [2].

II. LITERATURE SURVEY

Least Significant Bit (LSB) insertion [1, 2] is a common, simple approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image. The altered image is called steno-image.

To a computer, an image is simply a file that shows the different colours and intensities of light on different areas of an image. For hiding information inside images usually Least Significant Bit (LSB) method is used. In the LSB method, the 8th bit of every byte of the carrier file is substituted by one bit

of the secret information. This method works fine in the image carriers because if the least significant bit is changed from 0 to 1 or vice versa, there is hardly any change in the appearance of the colour of that pixel. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted, to overcome this problem we have introduced BPCS algorithm for embedding the data inside image, using this algorithm we can increase size of image which is a carrier to our secret data.

Researchers, for example El-Emma proposed a Steganographic algorithm to hide a large amount of data with high security. His Steganographic algorithm is based on hiding a large amount of data (image, audio, and text) file inside a colour bitmap (bmp) image. In his research, the image will be filtered and segmented where bits replacement is used on the appropriate pixels. These pixels are selected randomly rather than sequentially.Wu etal, on the other hand, used pixel-value differencing by partitioning the original image into non-overlapping blocks of two consecutive pixels.

This research uses a similar concept introduced by El-Emam. A bitmap (bmp) image will be used to hide the data. Data will be embedded inside the image using the pixels. Then the pixels of stego image can then be accessed back in order to retrieve back the hidden data inside the image. Two stages are involved. The first stage is to come up with a new steganography algorithm in order to hide the data inside the image and the second stage is to come up with a decryption algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stego image.

III. PROPOSED MODEL (ALGORITHM)

The proposed system model is shown in Fig. 1. The host image (cover image) is considered to with its maximum embedding capacity; while hidden source (secret information) is encoded using (hybrid cryptography) and then applied compression method is explained. After that embedded the secret information to the cover image using bit planes variance criterion. In hidden information encoder, 64 bits of the secret message is mapped to 8x8 binary noisy block of image.

As steganography algorithm is based on the image complexity on each bit plane, the secret key must include data about the exact mapping of secret information over the complex image. To determine if the complexity of determined region is enough for embedding, we use as reference a threshold value which is a function of the mean value of that region, and if the complexity of the region is greater or equal to this value, we deem that it is embeddable, and if not, the region is leaved alone. Based on this idea, a map with regions can be built complex enough to embed information for each bit plane. So that more information can be embedded in the cover image and no one can easily manage the attack to gain that information. At receiver site, first, the received stegoimage is decomposed to bit planes. Again, compute the complexity for each region on each bit plane and obtain a map with noisy regions. Of course, only those modified blocks of the image will hold the threshold used in the complexity computation process in the receiver. The obtained maps will contain the specific regions of the stego-image where the secret message was inserted. Once the blocks will have been extracted, the decomposer and decoder will make an inverse process to recover the message in its original format[7].

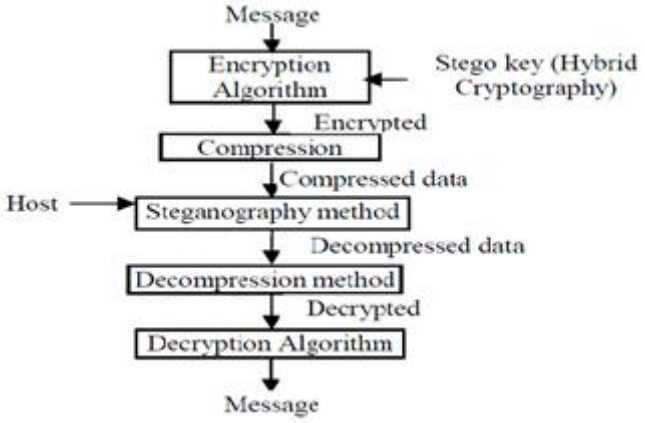


Fig. 1 Flowchart of proposed methodology

Process of encryption:

During process of encryption, data that we are going to encrypt is divided into data block of 4 columns of 4 bytes, which appears as 4*4 matrixes. In this we are using a user defined key, which is of length 128 bits. Encryption process undergoes 9/11/13 rounds in which state undergoes [6]:

- byte substitution (1 S-box used on every byte)
- shift rows (permute bytes between groups/columns)
- mix columns (subs using matrix multiply of groups)
- add round key (XOR state with key material)
- view as alternating XOR key & scramble data bytes

- Initial XOR key material & incomplete last round
- With fast XOR & table lookup implementation

Process of decryption:

- Process of AES decryption is not identical to encryption since steps discussed in reverse but can define an equivalent inverse cipher with steps as for encryption
  - but using inverses of each step discuss above
  - with a different key schedule
- Process works since result is unchanged when
  - swap byte substitution & shift rows

Swap mix columns & add (tweaked) round key **[6]**

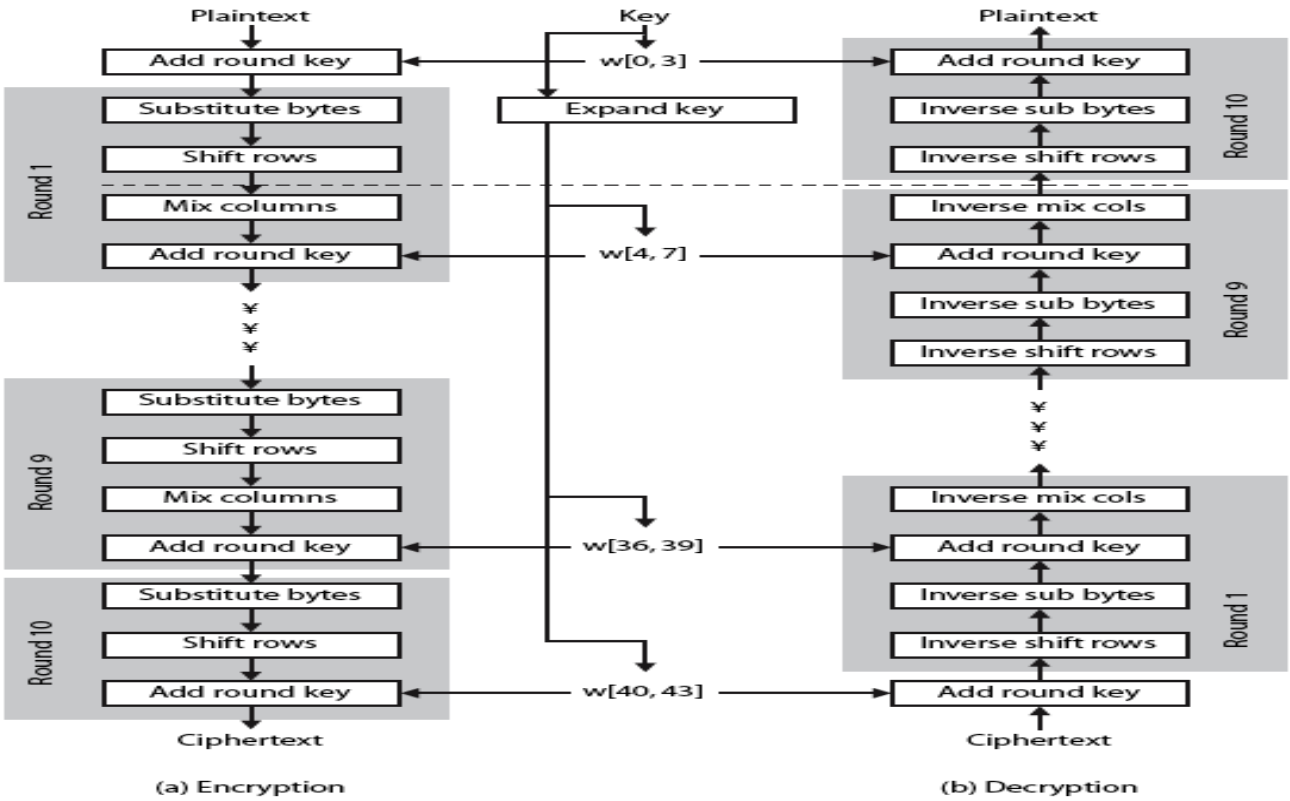


Fig. 2 Flowchart of encryption and decryption

BPCS Steganography:

The BPCS (Bit Plane Complexity Segmentation) technique is used to embed data into bitmap files. The ultimate goal is to embed as much data as possible into a cover image without detection by human perception or statistical analysis.

In BPCS, the noisy region of an image is located on each bit-plane as small pixel blocks which have noisy patterns. Each bit-plane of a container image is regularly divided into small

Square binary pixel blocks as illustrated in Fig. 3. A binary pixel block can be regarded as one in a noisy region if it has a complex black-and-white pattern. Only such complex blocks are used for embedding [8].

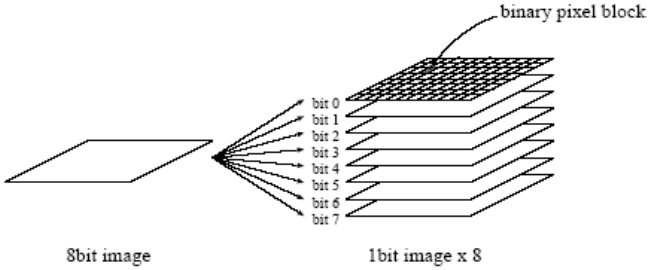


Fig. 3 Binary pixel blocks on bit-planes

The flowchart of BPCS Steganographic is shown in fig. 2, described as follows:

1. The carrier image is divided into 24 different Bit- Planes. All the bit-planes are divided into small pieces of the same size, which is called bit-plane blocks, such as 8 × 8 bits.

2. Calculate the complexity α of every block. The complexity is defined as the amount of all the adjacent pixels that get different values (one pixel is 0, and the other is 1).

3. Setting the complexity threshold of the bit-plane block is max *minAlpha* (customization parameter).

Here α is a parameter. The image complexity α is defined by the following.

α=k / (The max. possible B–W changes in the image) …… (1)

Where, k is the total length of black-and-white border in the image. So, the value ranges over

$0 \leq \alpha \leq 1$ ....…… (2)

Equation (1) is defined globally, i.e. α is calculated over the whole image area. It gives us the global complexity of a binary image. However, we can also use α for a local image complexity (e.g. an 8 × 8 pixel-size area). The bit-plane block

whose complexity is larger than minAlpha is used to embed secret information. The smaller the value of minAlpha, the more secret information can be embedded.

4. Secret information is formed into bit-plane blocks. The bit-plane block can replace the original one straightly if its complexity is greater than *minAlpha*. Yet, it needs to conjugate processing with the white checkerboard pattern block if the complexity of embedded block is less than or equal to *minAlpha*, then take the new block to replace the original one.

5. Make a record of the blocks that have taken conjugate processing and this information also need to be embedded into the cover image. The embeddings of this extra information cannot produce an effect on the embedded secrets, and it must be correctly picked up.

The process of secret information extraction is simple. Firstly, pick up all the pieces of the carrier data whose complexity is greater than *minAlpha*, and then pick up the extra embedded information mentioned in step (5) to confirm the blocks that have taken conjugate processing. These blocks need take XOR operation with white chess board block to get the recovery of secret.

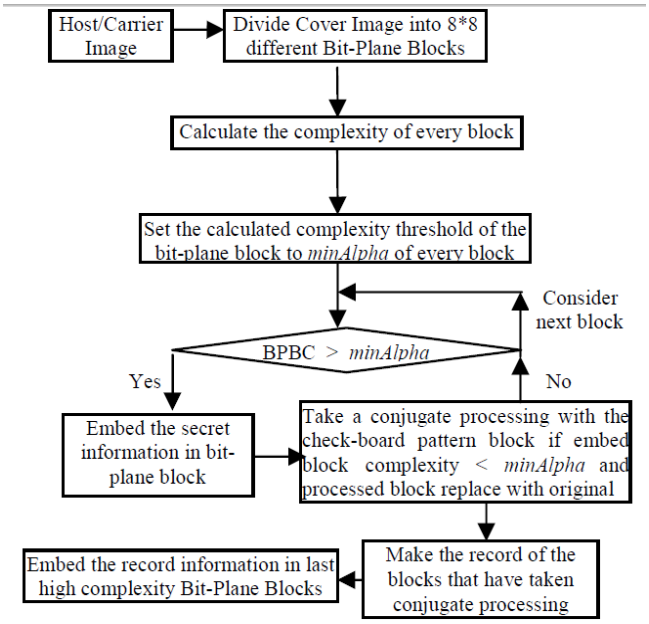


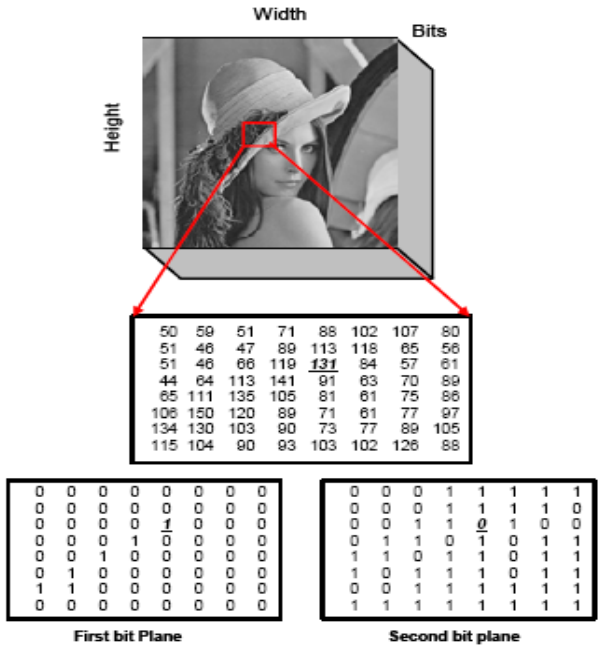
Fig. 4 Flowchart- Modified BPCS Steganography

The basic stegnography uses for bit 0, 1, 2 and 3. For bit 4, 5, 6 and 7; a new technique is used as: Apart from basic values of alpha (that is minimum complexity threshold), a new value
(Say gamma) is considered that indicate change in complexity from original 8*8 block of image to same stego image block. For 4, 5, 6 and 7 bit planes, first calculate alpha and if it is greater than minAlpha, then generate the bit pattern to be embedded from secret file and calculate alpha of the bit pattern as well.

Now after recalculating alpha for generated pattern and compare it with minAlpha, if smaller the alpha value, then take stegoimage and complex conjugate as in previous algorithm. Now calculate change in pattern from original image (i.e. changes in bits from original to modified imageblock). If this value (gamma) is less than minGamma, hide data in that calculated 8x8 blocks. If value is greater than minGamma of the block, then ignore that block for hiding purpose. The data can be hided in the block and use first two bits of block to indicate whether the bit pattern is conjugated and whether a valid data is indeed hidden or not. This way we can make use of entire image and increase the size of the data that can be hidden **[9]**

IV. EXPERIMENTAL RESULTS

Bit Plane Separation of image:



Ex. 131(10)=10000011(2)

The bit plane slicing can be better understood with the help of fig 2. The operation of splitting the image into its constituent binary planes is called “Bit plane slicing”[8]. Pixels are digital numbers composed of bits. In an 8-bit image, intensity of each pixel is represented by 8-bits. The 8-bit image is composed of eight 1-bit plane regions from bit plane ‘0’ (LSB) to bit-plane ‘7’ (MSB). Plane ‘0’ contains all lowest order bits of all pixels in the image while plane ‘7’ contains all higher order bits. Bit plane Slicing is useful for image compression. Complexity of each bit–plane pattern increases monotically from MSB to LSB[2].

V. FUTURE WORK

We are very convinced that this steganography is a very strong information security technique, especially when combined with encrypted embedded data. Furthermore, it can

be applied to areas other than secret communication. Future research will include the application to vessels other than 24-bit images, identifying and formalizing the customization parameters, and developing new applications.

CONCLUSION

Analysis has been conducted through number of observations by taking a wide variety of images from different sources. It provides two level security, encryption (hybrid Cryptography) and steganography. If at all the intruder suspects it is quite impossible for him to steal the data because embedding byte positions are decided based on modified BPCS approach. After the cipher text is embedded, the degradation in image quality is not apparent to normal human eye. Threshold is customaries; hence sender can decide data hiding capacity as well as quality of the image. This approach can be extendable to send secret images in carrier image.

This steganography is a strong information security technique, especially when combined with hybrid encrypted embedded data should be convinced. Furthermore, it can be applied to areas other than secret communication. Future research will include avoiding stegoanalysis by using analysis tools.

REFERENCES

[1] Behroz A. Forouzan, "Cryptography & Network Security", McGrawHill Publication,2008, New Delhi.
[2] M. S. Stone, M.V. Khan dare, "Image Based Steganography Using LSB Insertion Technique", Wireless, Mobile and Multimedia Networks ,IET International Conference, Jan-2008,pp-146 – 151
[3] Ross J. Anderson and Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE JOURNAL on selected areas in Communications, VOL. 16, NO. 4, MAY 1998, pp- 474 - 481.
[4]Babita Ahuja and Manpreet Kaur, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering,Vol. 1, No. 1, May 2009.
[5]Rafael C. Gonzalez, Richard E. Woods: Digital Image Processing, Third Edition, Pearson Education, pp. 117 – 119.
[6]Announcing the advanced encryption standard (aes)
[7] Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity
[8] BPCS Steganography Steve Beaullieu, Jon Crissey, Ian Smith University of Texas at San Antonio
[9] Principle and applications of BPCS-Steganography Eiji Kawaguchi* and Richard O. Eason** * Kyushu Institute of Technology, Kitakyushu, Japan ** University of Maine, Orono, Maine 04469-5708

