International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Steganography using PVD Algorithm for Android Application

D.Anandhavalli[1], C.Priyanka[2], N.Shanmuga Sundari[3], R.Kumaravalli[4],

[1&3] *Assistant Professor, Department of Information technology, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India.*

[2&4] *Student, B.Tech. Information technology, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India*

Abstract *–Information or any message hiding process encrypting into digital media for the purpose of security. Steganography is one such technique in which presence of secret message cannot be detected and we can use it as a tool for security purpose to transmit the confidential information in a secure way. The goal is to hide the message in such a way that no one apart from intended recipient even knows that the message has been sent. By combining steganography and encryption properties, it becomes harder for even the stego-analyst to regain the original text from the image. The pixel selection filter is used to obtain the best areas to hide information in the cover image to obtain a better rate. After that Message is hidden using Bit Replacement method. We also propose Pixel Value Differencing for implementing steganography. In spatial or frequency domain several Steganographic algorithms have been proposed for embedding data in digital images as cover media. Our proposed steganography with PVD provides better security through text.*

Key Words: *Steganography, pvd, pixel selection filter, stego-analyst*

1. INTRODUCTION

Now a day, many android applications are available which provides many smart things to the users. Google's Android Operating System in Mobile phones are still relatively new, however, Android Operating System has been progressing quite rapidly. Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography is very useful for information security. It may be influenced by many factors, such as the choice of cover object, the type of modification operation on cover elements, the number of embedding changes (related to the payload), and the distortion functions used to identify individual elements of cover that could be modified during embedding. Assume that the first three factors mentioned above are the same, designing the distortion function will be an important approach to minimizing the impact caused by embedding, and thus improve the security performance of steganography.

To minimize the impact caused by data embedding, the sender should choose to modify those elements (pixels/coefficients) in such a way that the caused detectable distortion is as small as possible. Embedding the secret message bits under the guidance of minimizing distortion function can improve the security performance of steganography and has been known for a long time. In presented the perturbed quantization (PQ) steganography. As a specific case, they pointed out that the sender can constrain the embedding changes to those DCT coefficients that experience the largest quantization error. Such kind of coefficients, when rounded to the other value, may leave the smallest embedding distortion.

In another two adaptive versions of PQ, i.e., texture-adaptive PQ (PQt) and energy-adaptive PQ (PQe) have been presented. Through considering the local block content such as texture complexity and energy capacity, JPEG steganography with higher security performance can be obtained. In, the authors have combined quantization step with quantization error in their distortion function to improve the security performance of JPEG steganography.

It presented another distortion function for JPEG steganography, which is called new PQ (NPQ). Three factors are considered, i.e., the quantization error, the quantization step and the magnitude of quantized DCT coefficients to be modified. Via nonlinearly combining these three different factors, the new distortion function, NPQ, can improve the security performance of JPEG steganography significantly. Designing steganographic algorithms for empirical cover sources, such as digital images, is very challenging due to the fundamental lack of accurate models. The most successful approach today avoids estimating the cover source distribution.

Instead, the steganography problem is formulated as source coding with fidelity constraint the sender embeds her message while minimizing an appropriately defined distortion. Practical algorithms that embed near the theoretical payload–distortion bound are available for a very general class of distortion functions. Within this framework, the only task left to the sender is essentially the design of the distortion function. In an attempt to relate distortion with statistical detectability, the authors of parametrized the distortion function and then searched for such values of the parameters that gave the smallest detectability evaluated as a margin between classes within a selected feature space (cover model).

However, unless the cover model is a complete statistical descriptor of the empirical source, such optimized schemes may, paradoxically, end up being more detectable if the Warden designs the detector "outside of the model", which brings us back to the main and rather difficult problem modeling the source. All of today's most secure steganographic schemes for digital images use heuristically defined distortion functions that constrain the embedding changes to those parts of the image that are difficult to model (e.g., complex textures or "noisy" areas). In the JPEG domain, by far the most successful approach is built around distortion functions that measure distortion with respect to the raw, uncompressed image.

The main advantage for using steganography is that hiding secret message behind an image so that no-one will suspect the file. Everyone will generally think it as an image so that the secret message will be transmitted without any suspicion. The image used to hide a message will be visible normally to human eye and no one will ever suspect just by looking the image. Hackers are everywhere and always try to intercept communication to get confidential data. By using Steganography, we can reduce the chance of data leakage. Even if the attacker gets access to your account or email, he will have no clue where the confidential message is hidden inside the image.

2. EXISTING SYSTEM

In the Existing System they provide binary image steganography scheme that aims to minimize the embedding distortion on the texture is presented. Given binary images are converted to vector pixels then Selecting the random pixel values secure image was stored into the pixel values. By using the existing system can hide the secured information's like medical data's behind the images. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [4].

Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [4]. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [5].

These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [6].

All of today's most secure steganographic schemes for digital images use heuristically defined distortion functions that constrain the embedding changes to those parts of the image that are difficult to model (e.g., complex textures or "noisy" areas). In the JPEG domain, by far the most successful approach is built around distortion functions that measure distortion w.r.t. the raw, uncompressed image. A natural way to define the distortion function in the spatial domain is to assign pixel costs by measuring the impact of changing each pixel in a feature (model) space using a weighted norm.

Making the weights dependent on the pixel's local neighborhood introduces desirable content adaptively. An example of this approach is the embedding algorithm HUGO, which employs the SPAM feature model. To the best knowledge of the authors, and based on the recent steganalysis study, HUGO is currently the most secure algorithm for embedding in the spatial domain even though its secure payload has been substantially lowered by modern attacks initiated during the BOSS competition that employ high-dimensional rich models. Three factors are considered, i.e., the quantization error, the quantization step and the magnitude of quantized DCT coefficients to be modified. Via nonlinearly combining these three different factors, the new distortion function, NPQ, can improve the security performance of JPEG steganography significantly.

Disadvantages

- ✓ Less security
- ✓ There is lot of chances to crypt analysis attacks.
- ✓ poor performance and it takes high amount of time for steganography process
- ✓ Cannot secure the Image data

3. PROPOSED SYSTEM

In our propose system, we provide the more advanced encryption standard for more advanced information standard process. Propose PVD standard encryption algorithms.Most of the Steganographic techniques use either three or four adjacent pixels around a target pixel so that imperceptibility value becomes high. PVD embedding is used for edged areas to increase image quality. It is also used to hide message into gray scale as well as in color image.

With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data.

Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 128 bits. Although there is a

complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors with large data caches. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. Also we propose LSB insertion method is the basic concept for image hiding techniques.

It embeds secret bits in LSB(s) of the cover image. A pixel which carries a fraction of secret data is called a target pixel. To find the most appropriate capacity value more surrounding pixels around a target pixel are utilized. LSB proves that discovering the best capacity value brings about an improvement in terms of imperceptibility. LSB embedding is used for smooth regions to increase capacity of hidden data. Most of the image hiding techniques use either three or four adjacent pixels around a target pixel so that imperceptibility value becomes high.

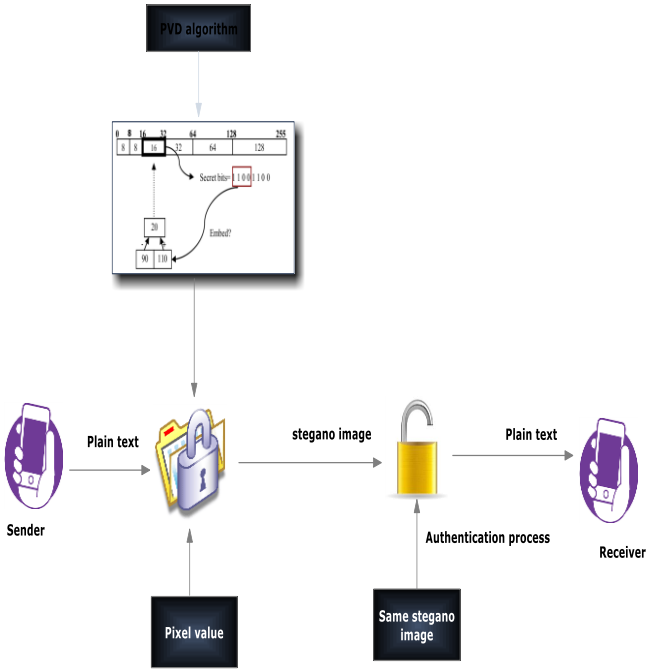

Fig-1: System Architecture

The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel. Monochrome and grey scale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color.

All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color are represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors. Not surprisingly the larger amount of colors that can be displayed, the larger the file size

Advantages

- ✓ Its more secure comparing than steganography method.
- ✓ It is the unbreakable security system.
- ✓ Can use this system for medical information's securing process.
- ✓ Asymmetric key encryption standard will provide the more security for information.

4. SYSTEM IMPLEMENTATION

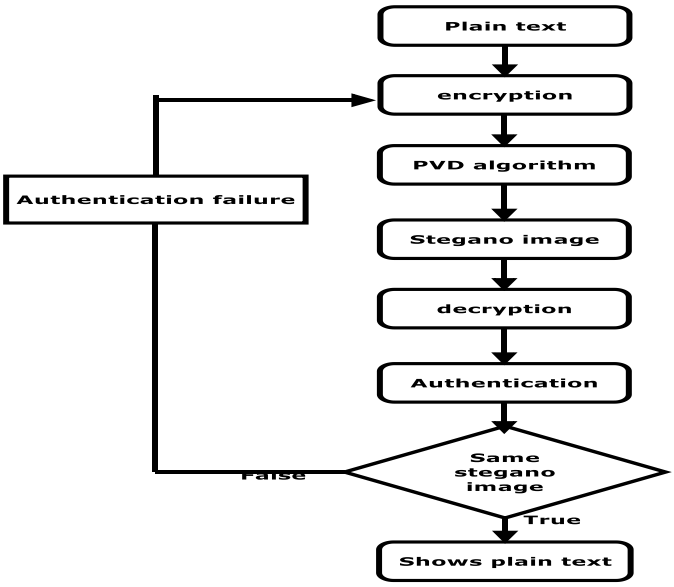

Fig-2: System Flow chart

4.1. ENCRYPTION STANDARD

Many encryption standard are available for encrypt the given text input. We use steganography based encryption standard which hide the text into image. Steganography is one of the most powerful techniques to dissemble the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Steganography and in this work image steganography is adopt-ed. In our first module we get input from text box. That inputted message is after converted to PVD manner.

4.2. TEXT HIDING

Text hiding is the method of hiding secure information behind the digital media like images. In the field of information secrecy it was the high authentic method. The advantage of steganography is that the intended secret message does not attract attention to itself as an object of scrutiny. In digital steganography, electronic communications may include cryptography coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganography transmission because of their large size.

4.3. PVD ALGORITHM

The PVD algorithm is able to provide a high quality stego image in addiction to high capacity of the concealed message. It can embed large amount of data without changing the consistency of the image quality. While embedding the secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. Then the corresponding difference value is calculated from the two pixels in each block. All possible difference values are classified into a number of ranges. The calculated difference value then replaced by a new value to embed the value of a sub-stream of the secret message.

4.4. DECRYPTION PROCESS

Decryption is a process of keeping secret messages hidden by which unauthorized users can't access that secret message. So, to hide the secured message encryption standard is used i.e transform plain - text into some other code called cipher - text and decryption is a reverse process of encryption i.e transform that cipher - text into original readable form. Only the same stegano image matches the receiver from which the message can be decrypted.

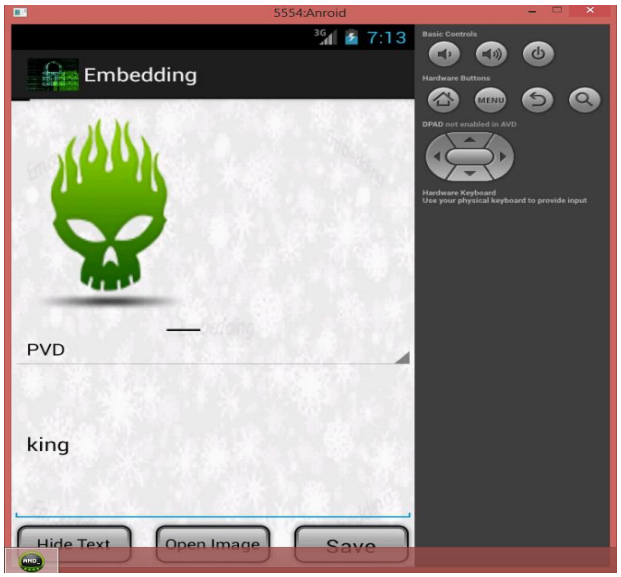

Fig-3: Embedding the text into the image

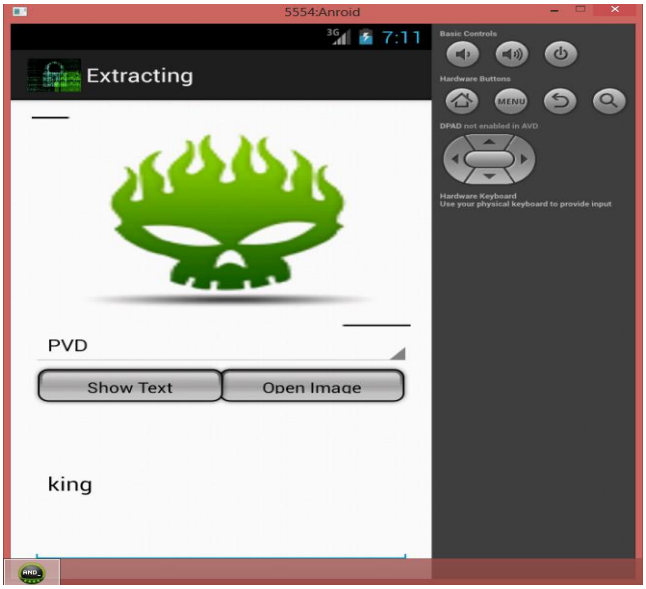

Fig-4: Extracting text from the image

5. CONCLUSION

The main goal of Steganography is to achieve secure communication. First encrypt a confidential file and then hide it inside an image before sending it to the destination hence it will decrease the chance of being intercept. While sending the file after encrypting, attacker will try to decrypt it by various ways. However, the attacker will only find a normal image file without any clue. This technique is very easy to use but very difficult to detect. Hence steganography can be used by government organizations for exchanging information securely.

REFERENCES

[1].F. Huang, W. Luo, J. Huang, and Y. Q. Shi, "Distortion function designing for JPEG steganography with uncompressed side-image," in Proc. 1st ACM Workshop Inf. Hiding Multimedia Security, 2013, pp. 69–76.

[2].K. L. Chiew and J. Pieprzyk, "Blind steganalysis: A countermeasure for binary image steganography," in Proc. Int. Conf. Availability, Rel. Security, Feb. 2010, pp. 653–658.

[3].T. Filler, J. Judas, and J. J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 920–935, Sep. 2011.

[4].Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," Proc. SPIE, vol. 4314, pp. 369–375, Aug. 2001.

[5].Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Trans. Commun., vol. 50, no. 8,pp. 1227–1231, Aug. 2002.

[6].M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.