ISSN:0975-9646

Utilization of Random Key and Sobel Filter based Edge Detection for Secure Data Transmission

Nithiyanantham Chandran
Department of Pervasive Computing Technology
Kings College of Engineering
Punalkulam, Pudukkottai, India

Arulkumar.S
Department of VLSI Design
Kings College of Engineering
Punalkulam, Pudukkottai, India

Abstract: In this cipher world, for sharing and exchanging purpose, the datas are need to travel from one end to another. To avoid cipher attacks and improve the confidentiality, the encryption and decryption techniques are needed. In this paper we offer nit procedure, a random key based stegnography techniques and also we approch a sophel filter for getting the image edges and mingle that values with random numbers (a kind of biometric encryption). This method restricts the Brute Force attack and the design might be suits for kit implementation.

Keywords: ***Cipher attacks; Encription; Decription; Shopel filter; stegnography***

I. INTRODUCTION

In simple words, Steganography can be defined as the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Though the concept of steganography and cryptography are the same, but still steganography differs from cryptography. Cryptography [1] focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. 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 the strength of steganography can thus be amplified by combining it with cryptography.

Steganography Imaging System (SIS) is a system that is capable of hiding the data inside the image. The system is using 2 layers of security in order to maintain data privacy. Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Privacy, on the other hand, is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively.
Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues. Data privacy issues can arise from a wide range of sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, residence and geographic records and ethnicity. Data security or data privacy has become increasingly important as more and more systems are connected to the Internet. There are informations privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, hiding the data in a kind of form such as within an image is vital in order to make sure that security or privacy of the important data is protected [2].

II. EXISTING SYSTEM

In an industrial point of view, the mobile operating system should consider as servant for a user and master for mobile components. The major mobile operating system such as Android, Bada, Blackberry, iPhone and Windows phones comes with built in features such as Bluetooth, Wi-fi, Gallery. These features also support or adapt with the new control coding.

A. Algorithmic based key generation

The system that should combine both public key, image and the text message. The key generation method is takes an important role of steganographic creation. Neither Advanced Encryptions Standard (AES) nor Data Encrption Standard (DES) algorithms are used here for generating the public keys. The AES take a deep effect for generating the keys because of preventing the brute force attacks. DES is a lightweight procedure; compare to AES, the security behavior will not meet the assured ability.
Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size [3].

A sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter

in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

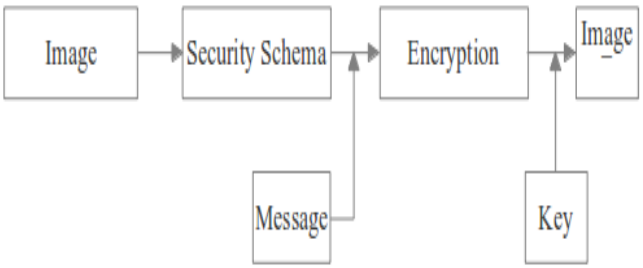

Fig 2.1 Steganographic Blocks

B**. Steganography in Digital**
Development following that was very slow, but has since taken off, going by the large number of steganography software available

- Concealing messages within the lowest bits of noisy images or sound files.
- Concealing data within encrypted data or within random data. The data to be concealed are first encrypted before being used to overwrite part of a much larger block of encrypted data or a block f random data (an unbreakable cipher like the One –time pad generates cipher texts that look perfectly random if one does not have the private key)

C. Steganography in Network
Typical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU (Protocol Data Unit), to the time relations between the exchanged PDUs, or both (hybrid methods).Moreover, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol steganography[4]. Hidden Communication System is a practical example of WLAN steganography system.

An alternative, there should be a partial encryption encrypts only a fracion of video data and improve the efficiency [8]. The scheme proposed in [9] encrypts the video cpdong(H.264/AVC) [8]. The video encryption is created with the help of IPM (intra-prediction mode) of intra macro blocks. Its security is analyzed in [5] followed with an improved scheme that encrypts not only for IPM but for Motion Vector Difference (MVD). Picture, intra-code frame, slice header and macroblock header of P-slice, and dc's are other video streaming parameters. But these ways are provided highly complexity and the cost for developing mechanism should increase mandatory.

III. Proposed System

The proposed system is an alternative and secure way of steganographic creation. The system has a preparation of public keys, and utilization of sobel filter for edge detection method. Here we recommend an ear image for having the biographic security, because which is definitely prevented the Brute force attacks.

A. Sobel Filter for ear edge detections
Sobel filtering is a three step process. Two 3 × 3 filters (often called kernels) are applied separately and independently. The weights these kernels apply to pixels in the 3 × 3 regions are depicted below,

-1	0	+1
-1	0	+2
-2	0	+1

+1	+2	+1
0	0	0
-1	-2	-1

Again, notice that in both cases, the sum of the weights is 0. The idea behind these two filters is to approximate the derivatives in x and y, respectively. Call the results of these two filters Dx (x, y) and Dy (x, y). Both Dx and Dy can have positive or negative values, so you need to add 0.5 so that a value of 0 corresponds to a middle gray in order to avoid clamping (to [0..1]) of these intermediate results[6].
The final step in the Sobel filter approximates the gradient magnitude based on the partial derivatives (Dx (x, y) and Dy (x, y)) from the previous steps. The gradient magnitude, which is the result of the Sobel Filter S(x, y), is simply,

$$S(x,y) = \text{sqrt}(Dx(x,y))2 + (Dy(x,y))2$$

The three steps for getting ear edges are,

- Compute the image storing partial derivatives in x (Dx (x, y)) by applying the right 3 × 3 kernels to the original input image.
- Compute the image storing partial derivatives in y (Dy (x, y)) by applying the left 3 × 3 kernels to the original input image.
- Compute the gradient magnitude S(x, y) based on Dx and Dy.

Two further things to notice about Sobel filters: (a) both the derivative kernels depicted above are separable, so they could be split into disjoint x and y passes, and (b) the entire filter can actually be implemented in a single-pass GLSL filter in a relatively straightforward manner [7].

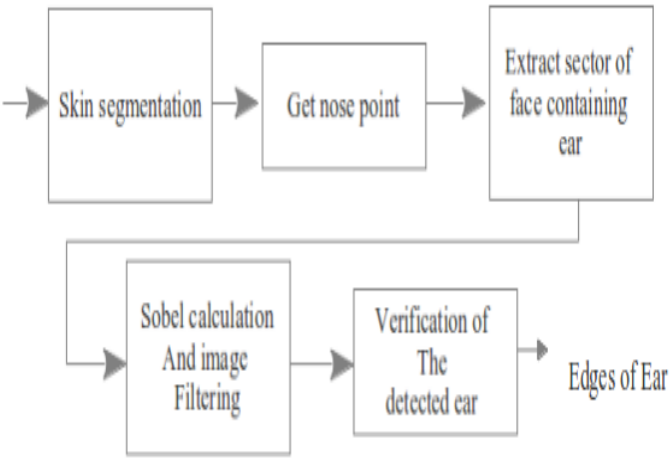

Fig 3.1 Getting edges of ear using Sobel Filter

B. Nit process

By using the above blocks the edges of an ear image (nit image) should be obtained. So the next proposal for encryption should describe with help of following block

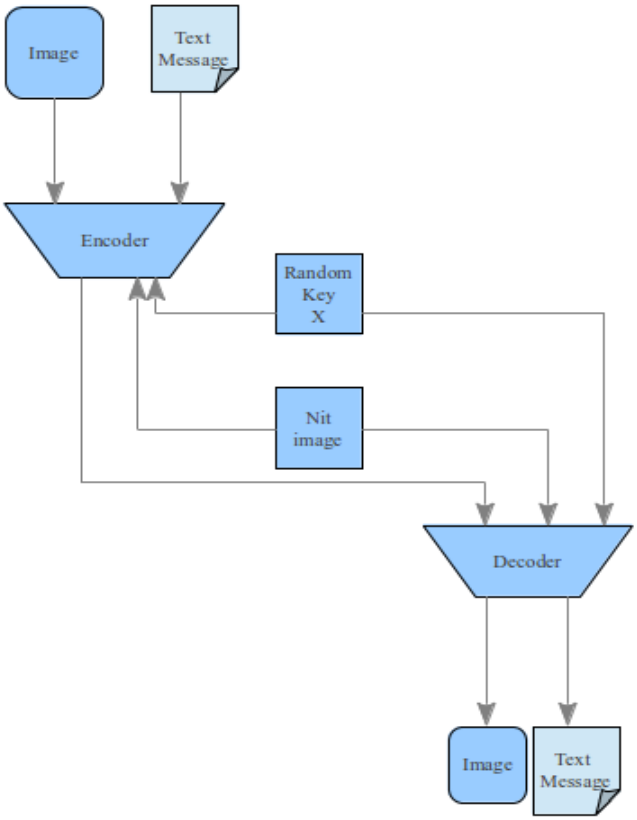

Fig. 3.2 Nit Process entire flow

The random key was generated with the help of random class or else the variable was assigned to the system timer. So an unpredictable number between two to n digit has been generated. That was assigned to that particular variable at once, at the same time the assigned image was declared as a global for inside the programming. Now the nit image, image as you want cryptographic, random key and text both values are added and the PNR was measured. The same reverse process has been held on decryption.

IV. Conclusion

If an attacker want to access with the help of key mean, most probable they will not aware of biographic image. As we conclude with the system advantages,

- It was a Lightweight process. There are no complicated programs.
- Provide high secure with low cost. Because compare to eye sensing it provide the same security with low cost.
- Easy to implement.

References

[1] N . Provos, "*Defending Against Statistical Steganography*," Proc 10th USENEX Security Symposium 2005.
[2] N . Provos and P. Honeyman, "*Hide and Seek: An introduction to Steganography*," IEEE Security & Privacy Journal 2003.
[3] Steganographic and image pixel ratings [june2013] http://en.wikipedia.org/wiki/steganographic
[4] Pixel and Process time [may 2013] http://en.wikipedia.org/wiki/onetime
[5] S. Lian, Z.,Liu,Z.,Ren and Z.,*Wang,"Selecive video encrption based on advanced video coding," in ProcPCM 2005 part II.*
[6] Sobel filtering [may 2013] http://en.wikipedia.org/wiki/sobel/
[7] PSNR calculation [june 2013] http://en.wikipedia.org/wiki/psnr
[8] *Advanced Video encoding.Final committee Draft,* Document JVT-E022, ITU-T Rec
[9] J.Ahn, H.Shim, B.Joen,and I.Choi,"*Digital video scrambling method using intra prediction mode,"* inProc. Vol 3333