A Dynamic Image Generation Scheme for Steganographic Data Encryption

Shahjada Imran Khan[1], Anindya Shankar Shukla[2], Anandarup Mukherjee[3]
[1]*(Dept. of Computer Science & Engg., University of Engineering &Management, Jaipur, India)*
[2,3]*(Dept. of Electronics & Communication Engg., University of Engineering &Management, Jaipur, India)*

Abstract: *This paper proposes a new approach to provide an extra layer of security to steganographic techniques. Today, most of the data is sent over the internet, whether personal or professional. Protection of digital multimedia content has become an increasingly important issue for content owners and service providers; therefore; there is a never ending demand to make the transmission network more secure. Conventional cryptography methods are vastly open to unauthorized attacks as they are well known to attackers and many new kinds of attacks are being raised, exploiting the loop holes in the conventional techniques. Hence, the demand for designing new techniques, for reliable encryption methods are high. This paper presents a novel method of hiding data in popular image formats like JPEG, TIF and PNG along with the message/data. The image in steganography till now, used to be fixed, standard images; we propose to implement dynamic images, which are generated using the user's voice. This kind of voice generated image is unique to each person and is virtually untraceable on the world wide web.*

Keywords: *Decryption, Encryption, Gray-scale image, Steganography, Voice recognition.*

I. Introduction

Steganography is the technique of conceal the data or information(image/sound/text) in other information(data/sound/image).Usually, it is defined as the artwork & sciences of writing hidden messages in such a manner that the message being hidden goes unnoticed to prying eyes, not familiar with the contents of the message. Trithemius in his treatise on cryptography and steganography, called Steganographia, which was disguised as a book of magic had the first recorded use of the term steganography. In the concurrent world we see there are lots of examples of unsecured use of internet, that is, any person can abuse the information that is being altered. To avoid this, the procedures such as Steganography, Cryptography and Watermarking were designed which are kinds of encryption of information [2].Here, the data is either changed from one form to other or just represented in dissimilar form and then forward over a network. Simple access to highly privileged information of a sound company/corporation and misuse of normal steganographic process are some of the great shortfalls in the current scenario. There is a very fine distinction between steganography and cryptology, which are frequently confused for one another, because both of them are used to protect and hide important information in plain sight. The dissimilarity between the two is that Steganography involves covering information so that it appears as if no information is hidden at all. If anyone views the image, in which the data is hidden, the person will fail to locate any trace of the message until he or she is absolutely certain about the method used for hiding the message and hence, the person will not be motivated enough to look for the data, let alone decrypt it. In the present day technical scenario, steganography relates to information or a file hidden inside a digital picture, audio or video file. Steganography essentially exploits the human perception as the human senses are not trained to look for files that have information hidden inside them. There are although, some programs which can check an image for hidden messages by analyzing sudden unnatural changes in the images by a process called steganalysis [3]. The sole benefit of Steganography over cryptography is its ability not to draw attention to meaasges hidden in images [5],[4] as noticeable encrypted messages, no matter how non-breakable will cause suspicion, and may be incriminating in some countries where encryption is unauthorized. Therefore, just as cryptography protects the contents of a message, steganography is said to protect both messages and communicating parties [1].

However, our work doesn't accurately fit to this definition because our objective is to protect the data/information from the attackers & make the information more secure over internet by adding an extra layer of security via voice. This paper attempts to give a fresh and novel approach to the art of steganography by making the images used for hiding messages, dynamic. The images are generated in response to a user speaking a certain phrase for certain duration of time. This dynamically generated image is used for steganographic purposes.

II. Methodology

This section presents the detailed steps in our approach to make steganography more untraceable. To test our approach, we have selected a random steganographic technique which uses LSB (Least significant bit) technique to hide data in images [6]. The procedure is explained below-

1.1 Input Message

The sender types a message or information. The message gets stored in a buffer. A random matrix is selected from a pool of character matrices. The position of each of the characters of that particular input message is found out from the character matrix. Here, the matrix dimension is mn, where n=number of rows and m=number of columns. As the matrix is 2 dimensional, each character generates two values, one for row number and the other for column. These are stored for further steps of encryption Encryption/Hiding the message a dynamically generated image.

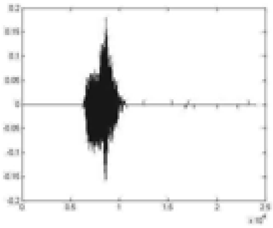


Figure 1: The plot of the voltage levels versus time, of a user's voice while repeating a pass-phrase. This plot is to be used as the cover image for hiding data.

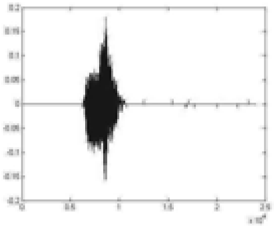


Figure 2: The cover image with the encrypted data.

1.2 Encryption

A voice is taken from the user uttering a particular phrase. It is converted to image by plotting its recorded voltage levels against time in a 2D plot, as shown in fig.1. The message to be hidden is encrypted in the image in such a manner that the resulting image is almost similar to the original cover image as seen in figs. 1 and 2. At the time of decryption, the user's voice uttering the same phase acts as the key to decrypt the message. The positions of the characters are converted to their respective binary values. The two values are concatenated into a single unit, representing a single character. The next step involves picking up a pixel value and converting it to binary. The first bit is taken and replaced with the binary bits of the positions found

Encryption Algorithm

Step 1: Record the voice of a user uttering a predefined and time limited phrase.

Step 2: Store the recorded voice and plot the variations in voltage levels of the recording with respect to time.

Step 3: The voice plotting is saved as .JPEG/.PNG/.TIF.

Step 4: convert the image to grayscale to simplify the computational load.

Step 5: Select any random character matrix from the matrix pool of m×n, where m is the number of Columns and n is the number of rows.

Step 7: Convert the positions in binary values and concatenate them for each character positions. The converted binary should be same in bit size for each position.

Step 8: Pick a pixel in a sequential manner and convert it to binary.

Step 9: Replace the binary values of positions with the least significant bit of the pixel's binary value

Step 10: Reconstruct the image by converting all the pixel values from binary to decimal to obtain the encrypted image.

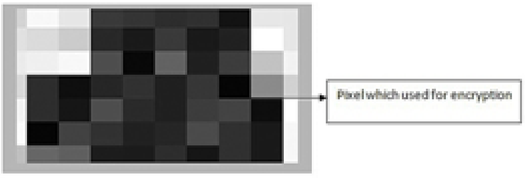


Figure 3: A snapshot of the pixel used for encryption in the actual image.

Previously (fig. 3). Subsequently, the binary number is converted to decimal value and replaced with the original pixel values. The main significance of this step is that it causes minimum change in a pixel value as the only change is in the LSB and it is either 1 or 0.

1.3 Decryption

When the receiver will go to decrypt the message he will be asked to enter the password to proceed. Here the password is the gray scale image of the recorded voice of the same phrase given by user. When the receiver will give the password it will check that the given password is right or wrong. If it doesn't match with the same password which is previously stored then it will show a message to the receiver that the password did not match & the process will be terminated. If the given password matches then it will reverse the encrypted process. There the selected matrix positions recovered by extracting those binary values & hidden position of the encrypted matrix doing some binary to decimal conversion. Then from the matrix pool will find out the hidden position of encrypted matrix which is previously stored & finally it will show up the original encrypted message.

Decryption Algorithm

Step1. Receiver speaks the original phrase, which is taken as a password.

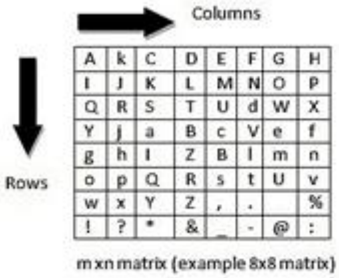
Step2 In case of non matching of phrase, the decryption process is terminated immediately.

Step3 If the password phrase matches, the decryption process starts.

Step4 The decryption process is simply the reverse of encryption process.

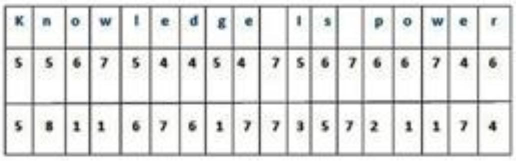
Step5 Position of the selected matrix is also recovered from the matrix pool.

Step6. After successful completion of decryption, the original message shows up.


Columns
Rows
m x n matrix (example 8x8 matrix)

A	k	C	D	E	F	G	H
I	J	K	L	M	N	O	P
Q	R	S	T	U	d	W	X
Y	j	a	B	c	V	e	f
g	h	I	Z	B	l	m	n
o	p	Q	R	s	t	U	v
w	x	Y	Z	,	.		%
!	?	*	&	_	-	@	:

Figure 4: A sample matrix used for generating the value of LSB (Least Significant Bit).



K	n	o	w	l	e	d	g	e		I	s		p	o	w	e	r
5	5	6	7	5	4	4	5	4	7	5	6	7	6	6	7	4	6
5	8	1	1	6	7	6	1	7	7	3	5	7	2	1	1	7	4

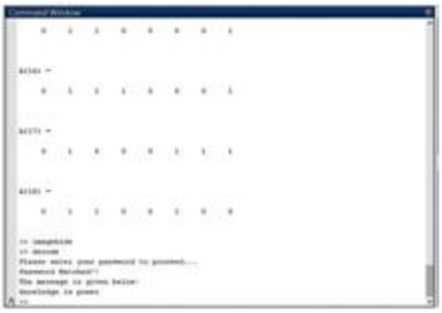
Figure 5: The secret message with its corresponding position in an encrypting matrix

III. Results

The proposed method in the previous section was applied in real time. The results and observations are tabulated and explained in this section. The verbal keyword, which is to be spoken, against which an image will be generated dynamically was taken as "Knowledge is power". A random matrix was selected for the LSB technique (fig.4). The message to be hidden was compared against the randomly selected matrix for determining the positions of the row and column of the corresponding alphabets in the selected matrix as shown in fig.5. For each character, an 8 bit binary value is generated where 4 bits of the binary sequence represent the column position and the remaining 4 bits, the row number.

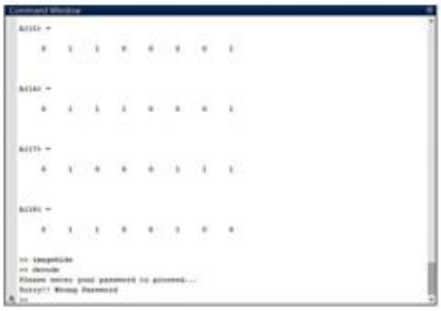
During decryption, when the receiver gives the password, this method checks the relation between the previously recorded voice & the recently uttered phrase. If the co-relation of two passwords or voices are near to unity or almost unity, the method immediately starts the decryption process; but if the co-relation between the two voices are poor or below our chosen threshold of 75% (0.75), the method then shows an error message to the receiver and terminates the decryption process as shown in the output windows in figs. 6 and 7.

To check the integrity of our method in hiding the message in image, we check the image compression quality of two similar images, one with the message hidden in it and the other without the message. The two methods to check for distortions in the images are MSE (Mean Squared Error) and PSNR (Peak Signal to Noise ratio). The MSE represents the cumulative squared error between the compressed or encrypted image and the original message, whereas PSNR represents the measure of the peak error. The lower the value of the MSE, the lower is the error. To compute the PSNR, the block first calculates the mean-squared error using equation 1 and puts it in equation 2. The following are the equations:



```
     0   1   1   0   0   0   0   1

a(16) =

     0   1   1   1   1   0   0   1

a(17) =

     0   1   0   0   0   1   1   1

a(18) =

     0   1   1   0   0   1   0   0

>> imagehide
>> decode
Please enter your password to proceed...
Password Matched!!
The message is given below:
knowledge is power
>>
```

Figure 6: A screenshot of the output screen when the voice password is matched.



```
a(13) =

     0   1   1   0   0   0   0   1

a(14) =

     0   1   1   1   0   0   0   1

a(17) =

     0   1   0   0   0   1   1   1

a(18) =

     0   1   1   0   0   1   0   0

>> imagehide
>> decode
Please enter your password to proceed...
Sorry!! Wrong Password
>>
```

Figure 7: A screenshot of the output screen when voice matching fails.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \{I(i,j) - K(i,j)\}^2 \qquad (1)$$

$$PSNR = 10 \log_{10} \left(\frac{Max_I{}^2}{MSE} \right) \qquad (2)$$

Where, m=number of rows in the image matrix, n =number of columns in the same matrix, I = the noise free image, K= noisy image, Max $_I$ = maximum possible pixel value of the image.

The calculated MSE value for the image is 3.1888e x 10^{-4} and its corresponding PSNR value is 83.0946.The calculated MSE value is very low, indicating a good quality image with very few errors. This indicates that the changes between the original image and encrypted image are very few and almost negligible, which makes our hidden message untraceable to prying eyes.

IV. Conclusion

This method can prove beneficial against hijacking, misuse and hacking of data through the internet. This process of sound steganography is better when compared to the present steganographic process [7].The method of converting a pass-phrase to voice signal and then converting the voice signal into an image to hide or encrypt data using conventional steganographic techniques provides a pretty strong encryption and obfuscation technique. This method can be easily used as an add-on to existing encryption techniques to add an extra layer of protection around the data they intend to encrypt. This would make the access of unauthorized users to encrypted data very challenging and virtually impossible to decrypt.

References

Journal Papers:

[1]. E. Winfree, and D. K. Gifford, "DNA Based Computers V, Massachusetts Institute of Technology," DIMACS Series in DiscreteMathematics and Theoretical Computer Science, American Mathematical Society, vol. 54, 2000.

Books:

[2]. W. Peter, "Disappearing cryptography: information hiding: steganography and watermarking," Amsterdam: MK/MorganKaufmannPublishers, 2002.

[3]. P. Fabian and A. P. Katzenbeisser, Stefan, "Information Hiding Techniques for Steganography and Digital Watermarking," ArtechHouse Publishers, 2000.

Chapters in Books:

[4]. S. Singh "The code book. The science of secrecy from ancient Egypt to quantum cryptography", SwiatKsiazki, pp. 19-21, 2003.

Online Resources:

[5]. N. Johnson, and S. Jajodia, “Steganalysis of Images Created Using Current Steganography Software,” Virginia, Fairfax. George Mason University. Center for Secure Information Systems.

Proceedings Papers:

[6]. Dipta Mukherjee, Anandarup Mukherjee, Somen Nayak, “A Hybrid Stegano- Cryptographic Approach to Data Obfuscation Using LSB Technique”, International Journal of Computer Applications, ISBN 978-81-923777-9-7, page 165-169,AUGUST, 2013.

[7]. S. Lyu and H. Farid, “Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines,” in Proc. 5th Int’l Workshop on Information Hiding, Springer-Verlag, 2002.