Open access Journal International journal of Emerging Trends in Science and Technology

Image Morphing with Data Security

Authors

Ankita Deshmukh *Thakur College of Engineering & Technology*

Priti Sharma *Thakur College of Engineering & Technology*

Anil Sahu *Thakur College of Engineering & Technology*

HarshaliPatil *Thakur College of Engineering & Technology*

ankitad1992@gmail.compriti@hg.ksanil@hg.ksharshali.patil@thakureducation.org

Abstract

Along with Computer and Network Security.Data Security plays a vital role in today world. Data is of great importance. In this paper, we have discussed how the data can be secured. This paper deals with hiding your encrypted data inside an image. Now this image would be covered by another image. We will apply some morphing techniques on these covered images to get morphed images. Now the morphed image is sent on the network. No one in the network can predict about data inside morphed images except the intended sender and receiver. This paper deals with three algorithms. The three algorithms are required for doing three different specific task. This paper deals with RSA algorithm for encrypting data .Second Water- marking embedding and extraction algorithm is used for hiding information inside image. And the third algorithm used is Hide and Extract image algorithm to cover your image behind other image

Keywords:
Least significant bits – LSB,
Cipher Text –C
Red Green Brown- RGB .

1. Introduction

We know that Information Security plays a vital role in ComputingEnvironment. To secure your Information the first idea we adopt is Cryptography.

Cryptography[1] is an art or science encompassing principle and methods of transforming message an intelligible into one that is unintelligible and then retransforming the message into original form. Usually, the encrypted messages look very unnatural. Some malicious person or group may just concentrate on the unnatural parts, and use all computing recourses to decrypt the messages. Thus, to make the information more secure, some other technology is required. An alternative technology is information hiding. Digital watermark and Steganography are two

representative technologies for information hiding. Information hiding is different from cryptography. The former tries to conceal the existence of the secret message, while the latter transforms the message to some understandable form. In fact, information hiding may protect the secret message better than cryptography because it is not easy for a malicious person to find what to attack. In information hiding, the secret message is embedded in some unrelated cover message. The cover message in which the secret message is embedded is called stego data in steganography. To ensure the security, it is crucial to keep the stegodata as close as the cover message, or the existence of the secret message can be detected easily[2]. Currently, we proposed a new information hiding technique based on image morphing. Originally, image morphing is the process to change one image (the source image) to another (the target image) smoothly. The morphed image is a intermediate image produced in the morphing process looks like a natural image, and some of them can actually be used as the stegodata. In this paper, we call an intermediate image the morphed image. Clearly, both the source image and the target image can be hidden in the morphed image. Since the morphed image is similar to the source image and the target image, it may not be secure if we try to hide two images together. Thus, we just consider to use one image (e.g. the source image) as the secret image, and use another (e.g. the target image) as the cover image. To ensure the security, the cover image is used as one of the stego keys, and is kept secretly.

In the morphing based technique, instead of trying to keep the stegodata close to the cover message, we just try to keep the naturalness of the stegodata[2]. The most significant advantage of this relaxation is that we can increase the cover rate. An image can cover anotherimage of the same size. However , the problem to hide face images, and applied the morphing based technique for protecting the privacy contained in a face database. However, there are two fatal problems in the morphing based technique. First, the morphed image may not look natural due to inaccurate definition of the feature lines or feature points. Second, the secret image can be estimated to some extent from the stegodata. In this paper, we propose several methods for solving the above two problems. Specifically, to solve the first problem, we propose to scale down the secret message before calculating the morphed image. To solve the second problem, we propose to encrypt the secret message first, and then hide it to the warped cover image. To increase the security further, we also propose to separate the stego key and the secret message. These methods can make the morphing based technique much more practically useful.

The main aim of the paper is to develop system that processes a text message by encrypting it and then hiding it behind an image This image is further processed i.e image morphing is performed so as to enhance the security provided to the message.

2. RSA

RSA is one of the algorithms widely used for encrypting data. It is a asymmetric cryptography. The algorithm goes its name from the initial of its inventor **R**ivest, **S**hamir &**A**dleman. This algorithm makes use pair of keys. The one key is public and other key is private. The public key is known to everyone and is used for encrypting data. While the private key is known only to receiver and is used for decrypting the data.This algorithm make use of large integers.based on exponentiation in a finite (Galois) field over integers modulo a prime.[1] This algorithm work as follows

1. Select two large primes at random - p, q.
2. Compute the system modulus n =p*q.

3. Calculate the toluent factor as ø(n)=(p-1)(q-1).
4. Select at random Encryption key e such that it Satisfy the given condition gcd(e,ø(n))=1
5. To find decryption key, solve the given below equation e.d=1 mod ø(n) and 0≤d≤n.
Hence, public Encryption key = {e, n}.
And the private Decryption key = {d, n}.
Thus , the message M can be encrypted as
Cipher Text $C=M^e$ mod n.
And the original message M can be obtained using
Original Message $M=C^d$ mod n.

3.WaterMarking Embedding and Extraction Algorithm

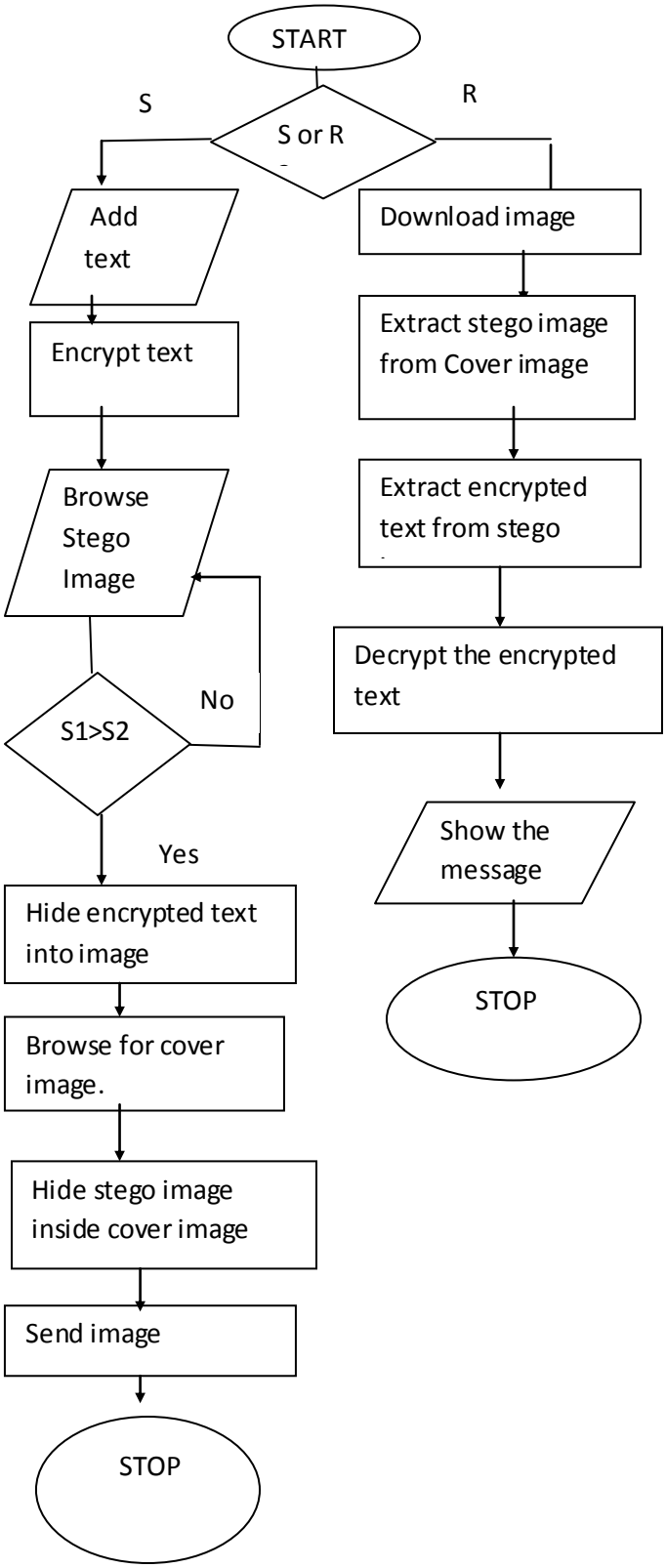
Digital watermarking[3,4] is a technique for inserting information (the watermark) into an image, which can be later extracted or detected for variety of purposes including identification and authentication purposes.
Imperceptible to human senses, Digimarc's digital [3,4]watermarking technology allows users to embed digital information into audio, images, video and printed materials in a way that is persistent, imperceptible and easily detected by computers and digital devices.
We make use of first WaterMarking Embedding algorithm to hide information inside images
Load image
Define starting watermark payload as zero bits
Conversion RGB -> YCbCr
Extract Y, Cb, Cr components
Create LSB matrix for Cb and Cr components
mod(component,2)
Embed bits in blocks 25x25
If current bit is 1, then LSB of Cb is 0 and LSB of Cr is 1
cb=cb-lsbits_cb
cr=cr-lsbits_cr+1
If current embed bit is 0, then LSB of Cb is 1 and LSB of Cr is 0
Opposite scheme in adjacent blocks
Create result image
Conversion YCbCr -> RGB
Save result file
Now we make use of WaterMarking Extraction algorithm to extract information From images
Define starting watermark payload as zero bits
Conversion RGB -> YCbCr
Extract Y, Cb, Cr components
Create LSB matrix for Cb and Cr components
Read image in blocks 25x25
lsbits_cb()<2
Decision of watermark bit value in current block
Move to next position in watermark
Reset counters
Conversion of binary form of watermark to text displayed in text area

4. Hide and Extract Image Algorithm

Once the information is been hidden inside image. We need to cover these images by another images known as Covered image.[5,6]
We make use of Hide Image algorithm first
Extract cover image information.
Extract cover image height and width.
Get the red color matrix.
Extract the secret image height and width from 1st 32pixel of cover image.
Initialize a zero matrix.
Set counter for pixels.
Extract the secret image from the cover image
Now we make use of Extract Image algorithm
Extract cover image information.
Extract cover image height and width.
Get the red color matrix.
Extract the secret image height and width from 1st 32pixel of cover image.
Initialize a zero matrix.
Set counter for pixels.
Extract the secret image from the cover image.

4.1Diagrammatic Representation

Here is a quick informal explanation of all the Process explained above. This flow Chart Guides all the activities that should be carried out from Sender as well as Receiver side .



5. CONCLUSION

This paper deals with the image morphing based information hiding technology briefly. The flow diagram of this technique is shown in Fig. 1. First of all, to hide a secret image through morphing, we should define some features (points or lines) in the secret image and the cover image. We also need to define the morphing rate. With these stego keys, we can combine the secretimage and the cover image through morphing, and get the morphed image. The morphed image will be used as the stegodata, and be transmitted to the authorized person through public channel. Upon receiving the morphed image, the authorized person can reconstruct the secret image through de-morphing using the same stego keys, which are sent to the authorized person in advance through some secret channel. The basic idea of the morphing based information hiding technique is to protect the secret message (e.g. a face image) by transmitting or storing the morphed image, which is one of the intermediate images produced in the morphing process. In fact, the morphed image can be produced directly if the morphing rate is given. The point is, if the morphed image looks natural, it will be difficult to know the existence of the of the secret message.

REFRENCES

[1]The Mathematics of the RSA Public-Key Cryptosystem by Burt Kaliski .
[2] TCP/IP protocol suite by Behrouz.A.Forouzan.
[3] Research on Fast implementation of RSA with java, Proceedings of 2010 International Symposium on Web Information System and Application (WISA'10).
[4] Gonzalez And Woods .Digital Image Processing.
[5] Digital Image Processing by W. K. Pratt.
[6] Fundamentals of Digital Image Processing by A.K. Jain.