IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.
www.ijiset.com
ISSN 2348 – 7968

Encryption of Data Behind The Diverged Audio And Video Frame Using RSA Algorithm

Mrs.K.Brindavathi[1], Mrs.B.Oviya[2]

[1,2] PG student, Sri manakula vinayagar engineering college,puducherry,

ABSTRACT:

From the existing level of encryption data processing, system cannot find out the encryption of data under the divergent of audio as well as video scenario. Hence, system have to put-forth the process of the divergent manner of audio as well as video frame diverging and so (hiding the encrypted data under the frame).

In the present day secure data transmission is needed due to attack made on data communication from one end to other end. This paper provides the technique to overcome the above requirements. In this proposed method the data is transmitted by encrypting it and hiding it behind the diverged audio and video frame. Video steganography uses video as cover media for embedding secret data. RSA based algorithm scheme has been used as a base technique for hiding the encrypted text in the diverged audio and video frame. In the receiver side the original data will be received by decrypting the hidden text in the diverged frame.

Keywords: Encryption; video steganography; diverged audio and video frame; decrypted data.

INTRODUCTION:

Cryptography and Steganography are well known and widely used techniques, in that Steganography is the art and science of communication in a way which hides the existence of the communication manipulate information (message) in order to cipher or hide their existence respectively.

Cryptography scrambles a message it cannot be understood; the Steganography hides the message so it cannot be seen. In this paper we will focus to develop one system, which uses both Cryptography and Steganography for better confidentiality and security. Even though these two techniques are straight forwardly, there is a chance that the intruder may detect the original message. Therefore the proposed system apply both of them together with more security levels and to get a very highly secured system for data hiding.

This paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography. As we know that-

- Hiding data is better than moving it shown and encrypted.
- To hide data in a popular object that will not attract any attention.
- In case the data is extracted, it will be encrypted one.

But still there is a chance that the intruder can break the code. In our new system instead of applying existing techniques directly we will using the following approach-

- Instead of hiding the complete encrypted text into an image, the proposed system is hiding a part of the encrypted text in a extracted and selected video frame.
- Unhidden part of the encrypted message will be converted into two secret keys.
- To get the original message one should know, along with keys for Cryptography and Steganography, two extra keys and reverse process of the key generation.

ISSN 2348 – 7968

BACKGROUND STUDY

Steganography based information hiding:

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. Steganography is a technique of hiding information in digital media. In contrast to cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video, and images. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use.

The word steganography comes from the Greek Steganos, which mean covered or secret, and –stegnography mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening. Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed. Until recently, information hiding techniques received very much less attention from the researchcommunity and from industry than cryptography. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996. There has been a rapid growth of interest in steganography for two main reasons.

- The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.
- Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

Methodology

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are including:

(i) Least significant bit insertion (LSB)

(ii)Masking and filtering

(iii)Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the

ISSN 2348 – 7968

least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

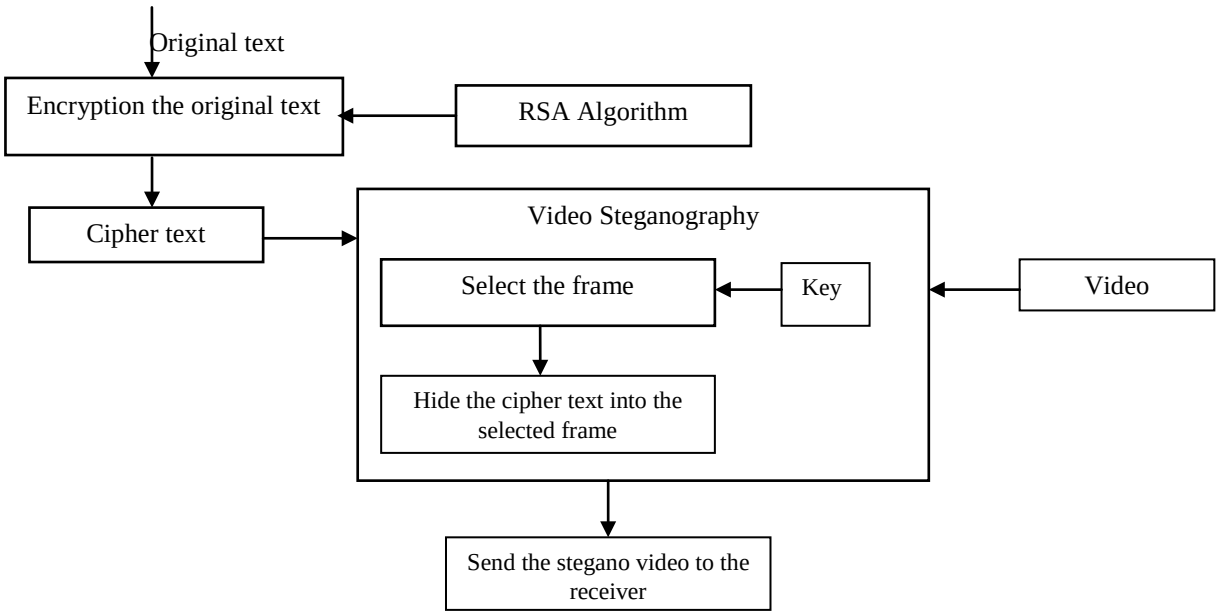
Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level. Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack.

PROPOSED SYSTEM

The block diagram of proposed data hiding is shown in the Fig.a. In the proposed system a secret message is hidden in the diverged audio and video frame by using secured **RSA** algorithm. The paper proposes two methods using LSB coding along with encryption to hide information (audio, image and text) in digital audio files. In the first method, the information is hidden by altering LSBs indirectly considering parity of samples of cover audio. In the second method, information is hidden by performing XOR operation on LSBs. In both these methods, direct LSB extraction will only result in noise. Thus, by using encryption along with steganography, these methods provide an additional level of security. From experimental results, it is seen that the proposed methods are effective. From listening tests, no difference is found between the original audio signal and thestego audio signal. The hidden information is recovered without any error. A novel idea which is an extension to the second proposed method based on XORing of LSBs that uses multiple LSBs has also been presented. This approach increases the capacity of the cover audio by as much as 8 times and also provides robust encryption. This will give great security and the embedded message cannot be extracted without the knowledge of the embedding process

SYSTEM IMPLEMENTATION

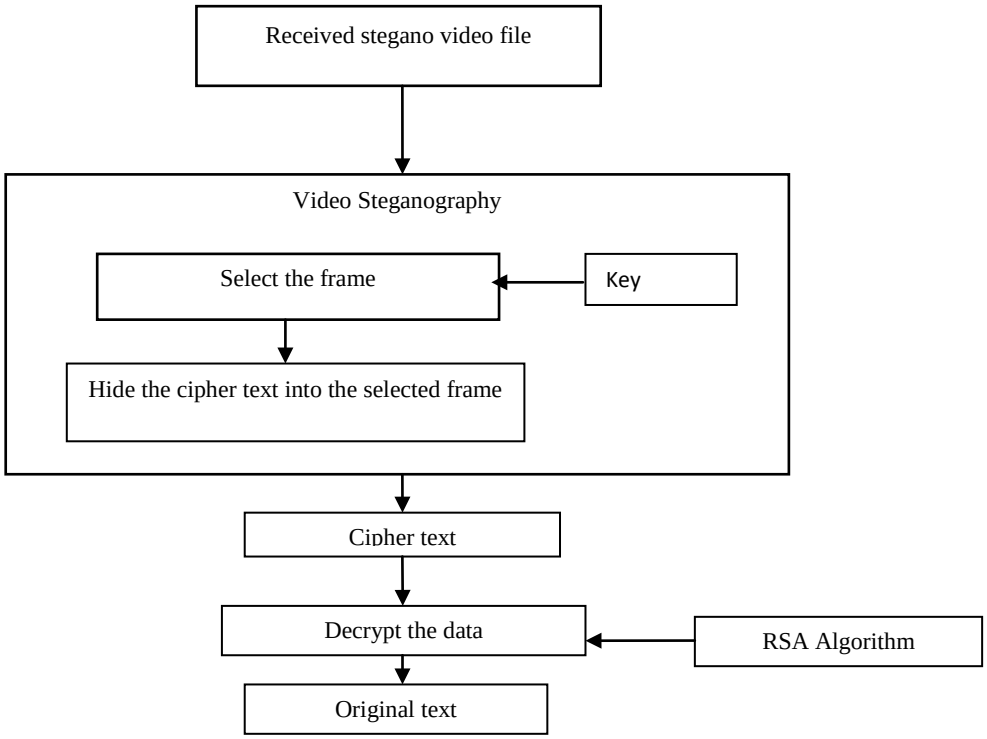
SENDER



(A). Sending the stegano video to the receiver

ISSN 2348 – 7968

RECEIVER



(B).Receiving the stegano video from the sender

Algorithm

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers p and q
2. Calculate $n = pq$
   - n is the modulus for the public key and the private keys
3. Calculate the totient: $\phi(n) = (p-1)(q-1)$.
4. Choose an integer e such that $1 < e < \phi(n)$, and e is coprime to $\phi(n)$ **ie:** e and $\phi(n)$ share no factors other than 1; gcd(e,$\phi(n)$) = 1.
   - e is released as the public key exponent
5. Compute d to satisfy the congruence relation $de \equiv 1 \pmod{\phi(n)}$ **ie:** $de = 1 + k\phi(n)$ for some integer k.
   - d is kept as the private key exponent

Notes on the above steps:

- Step 1: Numbers can be probabilistically tested for primality.
- Step2: changed in PKCS#1 v2.0 to $\lambda(n) = \operatorname{lcm}(p-1, q-1)$ instead of $\phi(n) = (p-1)(q-1)$.

ISSN 2348 – 7968

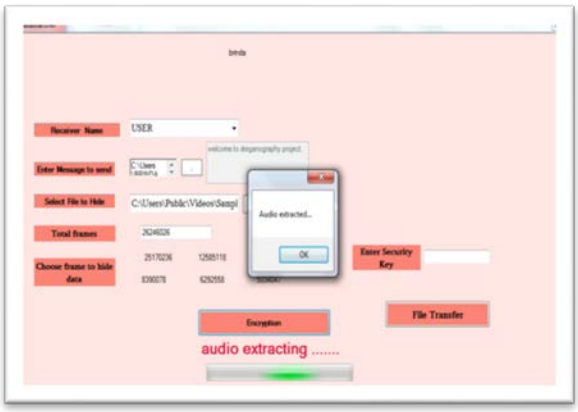
- Step 4: A popular choice for the public exponents is $e = 2^{16} + 1 = 65537$. Some applications choose smaller values such as $e = 3$, 5, or 35 instead. This is done to make encryption and signature verification faster on small devices like smart cards but small public exponents may lead to greater security risks.
- Steps 4 and 5 can be performed with the extended Euclidean algorithm; see modular arithmetic.

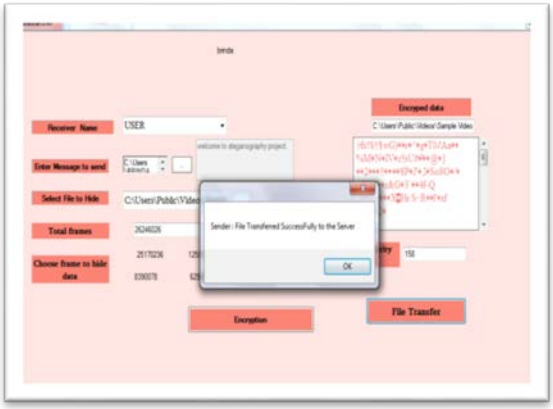
The **public key** is made of the modulus n and the public (or encryption) exponent e. The **private key** is made of the modulus n and the private (or decryption) exponent d which must be kept secret.

- For efficiency a different form of the **private key** can be stored:
  - p and q: the primes from the key generation,
  - $d \mod (p-1)$ and $d \mod (q-1)$: often called *dmp1* and *dmq1*.
  - $q^{-1} \mod (p)$: often called *iqmp*
- All parts of the private key must be kept secret in this form. p and q are sensitive since they are the factors of n, and allow computation of d given e. If p and q are not stored in this form of the private key then they are securely deleted along with other intermediate values from key generation.
- Although this form allows faster decryption and signing by using the Chinese Remainder Theorem (CRT) it is considerably less secure since it enables side channel attacks. This is a particular problem if implemented on smartcards, which benefit most from the improved efficiency. (Start with $y = x^e \pmod n$ and let the card decrypt that. So it computes $y^d \pmod p$ or $y^d \pmod q$ whose results give some value z. Now, induce an error in one of the computations. Then $\gcd(z - x, n)$ will reveal $p$or q.)

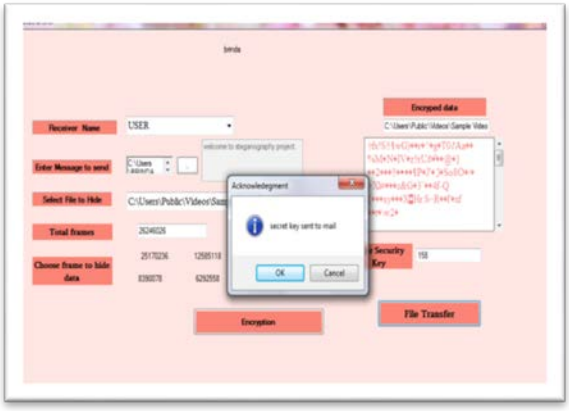
SCREEN SHOT

SENDER

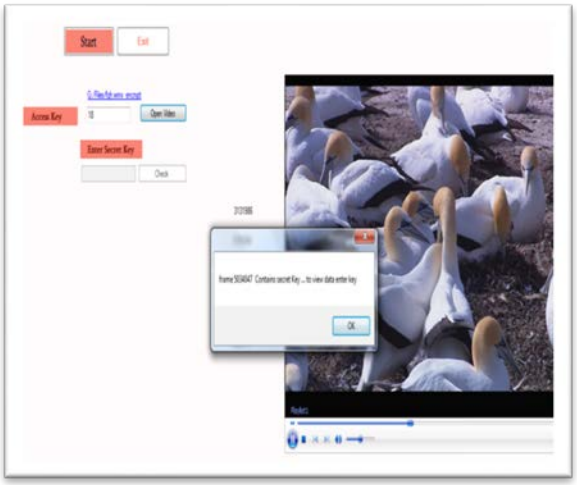


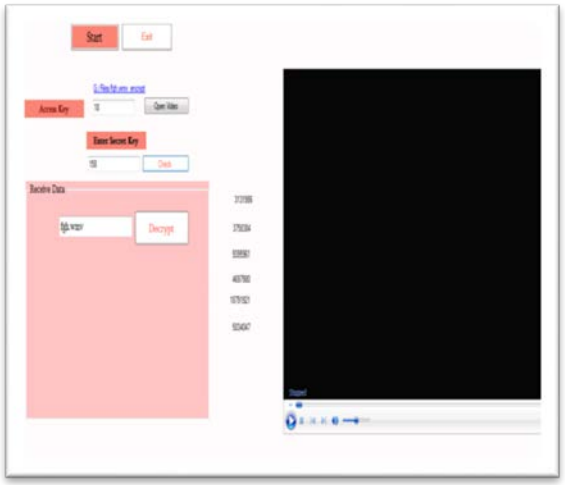


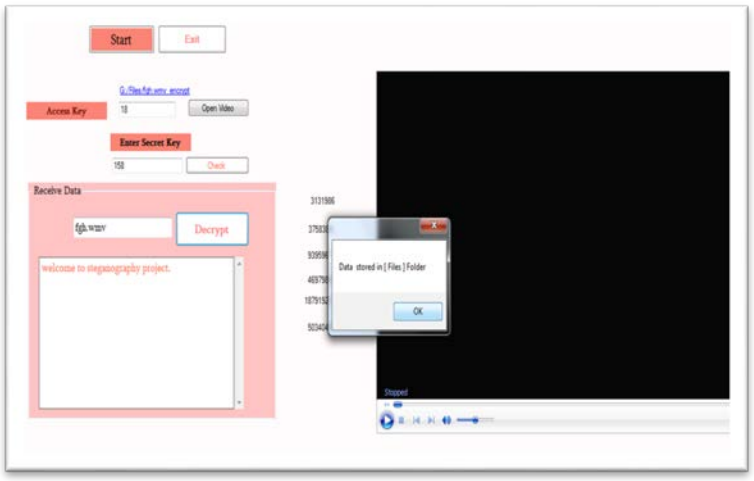
ISSN 2348 – 7968



RECEIVER







CONCLUSION

Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. This paper we have presented an enhancement of the video steganographic system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the video. In

ISSN 2348 – 7968

our proposed approach, the message bits are embedded randomly into the video instead of sequentially. We pointed out the enhancement of the audio steganographic system using LSB approach to provide a means of secure communication. Finally, we have shown that steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message.

REFERENCES

1. Yanyan Xu, "A content security protection scheme in JPEG compressed domain", in visual communication image representaiton, J.Vis.Commun.Image R.25,805–813,2014.
2. Saiful Islam, Phalguni Gupta, "Effect of morphing on embedding capacity and embedding efficiency", Neurocomputing 137 (2014) 136–141.
3. Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz, G.M. Bhat," Data hiding in scrambled images: A new double layer security", Computers and Electrical Engineering 40 (2014) 70–82
4. Dora M. Ballesteros L,Juan M. Moreno A," Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key", Computers and Electrical Engineering 39 (2013) 1192–1203
5. A. Boho, G. Wallendael, A. Dooms, J. Cock, G. Braeckman, P. Schelkens, B. Preneel, R. Walle, End-To-End security for video distribution, the combination of encryption, watermarking, and video adaptation, IEEE Signal Process. Mag. 30 (2) (2013).
6. A.V. Subramanyam, Sabu Emmanuel, Mohan S. Kankanhalli, Robust watermarking of compressed and encrypted JPEG2000 images, IEEE Trans. Multimedia 14 (3) (2012) 703–716
7. Chia-Chun Wua, Shang-Juh Kao, Min-ShiangHwangb," A high quality image sharing with steganography and adaptive authentication scheme", The Journal of Systems and Software 84 (2011) 2196– 2207
8. Jordi. Serra-Ruiz, David. Megias, A novel semi-fragile forensic watermarking scheme for remote sensing images, Int. J. Remote Sens. 32 (19) (2011) 5583–5606
9. [3] Hermann Hellwagner, Robert Kuschnig, Thomas Stu ¨tz, Andreas Uhl, "Efficient in-network adaptation of encrypted H.264/SVC content,"SignalProcessing:Image Communication 24 (2009) 740–758.
10. Lathikanandini. M, Suresh. J," Steganography in MPEG Video Files using MACROBLOCKS", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-1 Issue-8 March-2013
11. KousikDasgupta, Jyotsna Kumar Mondal, Paramartha Dutta," Optimized Video Steganography using Genetic Algorithm (GA)", International Conference on Computational Intelligence: Modeling, Techniques and Applications, Proc Technology 10 (2013) 131 – 137.