RESEARCH ARTICLE OPEN ACCESS

An Modified Enhanced Method of Reversible Data Hiding In Audio Encryption

Dr.M.Kavitha* PL. Natchiammai **
[*] *Professor, , Mookambigai College of Engineering, Pudukkottai, Tamilnadu, India.*
*Kavitha79ramar@gmail.com **Assistant Professor, Electronics & Communication Engineering Department, Mookambigai College of Engineering, Pudukkottai, Tamilnadu, India.*

ABSTRACT:
Recently more & more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original data can be recovered after embedded data is extracted. It protects the image content. The proposed method is data embedded in encrypted audio file. The proposed chaotic encryption technique encrypts the audio file and then encrypted data will be embedded into encrypted audio file. This algorithm provides high level security. Using reversible data hiding algorithm, data is embedding in encrypted audio. The data hiding technique uses the least significant bit replacement algorithm for concealing the secret message bits into the encrypted audio. This important technology is widely used in defence & law forensics where no distortion of the original cover is allowed. In decryption, secret encrypted data will recover from encrypted audio file and then original audio file is extracted.

Keywords: Reversible data hiding, audio encryption, chaos, security

---

Date of Submission: 20-07-2017 Date of acceptance: 14-08-2017

I. INTRODUCTION

Steganography is that the art and science of writing hidden messages in such a way that nobody, except for the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and suggests that "concealed writing" from the Greek words steganos which means "covered or protected", and graphein which means "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a writing on cryptography and steganography disguised as a book on magic.

The advantage of steganography over cryptography alone is that messages don't attract attention to themselves. Plainly visible encrypted messages no matter however unbreakable will arouse suspicion, and may in themselves be incriminating in countries wherever cryptography is against the law. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

In a computer-based audio Steganography system, secret messages are embedded in digital sound. the key message is embedded by slightly sterilisation the binary sequence of a sound file. Existing audio Steganography software system will embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is sometimes a tougher method than embedding messages in alternative media, like digital images.

Proposed methodology introduces a brand new methodology of embedding secret data within skin because it isn't that much sensitive to HVS (Human Visual System).This takes advantage of biometrics features such as skin tone, rather than embedding data anyplace in image, data are embedded in selected regions. Summary of methodology is in short introduced as follows. Initially skin tone detection is performed on input image (Hue, saturation, value) color space. Secondly cover image is transformed in frequency domain. This can be performed by applying Haar-DWT, the best DWT on image resulting in four sub subbands. Then payload (number of bits within which we are able to hide data) is calculated. Finally secret knowledge embedding is performed in one amongst the high frequency sub-band by tracing skin pixels in that band.

In theoretical aspect, **Kalker and Willems[1] established a rate-distortion model for RDH**, through which they proved the rate-distortion bounds of RDH for memoryless covers and proposed a recursive code construction which however does not approach the bound.

Capacity-approaching codes for reversible data hiding was planned by Zhang Chen and Yu[2]. This paper improved the

algorithmic code construction for binary covers and tested that this construction are able to do the rate-distortion certain as long because the compression formula reaches entropy, that establishes the equivalence between knowledge compression and RDH for binary covers. It proposes associate degree improved algorithmic construction, associate degree improved cryptography for all-zero cover and a reversible data hiding methodology for binary cover.

Lossless data embedding for all image formats was planned by Fridrich and Goljian [3] proposed a an approach of a general framework for RDH techniques. By initial extracting compressible options of original cover then press them losslessly, spare space may be saved for embedding auxiliary data.

Reversible data embedding using a difference expansion was planned by Tian J [4]. A lot of widespread methodology is predicated on difference expansion(DE), during which the distinction of every pixel cluster is enlarged, e.g., increased by a pair of, and therefore the least significant bits of the difference are all-zero and might be used for embedding messages. **Separable reversible data hiding in encrypted images was proposed by Zhang [5],** a unique theme for seperable reversible data hiding in encrypted images. In the initial section, a content owner encrypts the first uncompressed image mistreatment associate degree secret writing key. Then a data-hider could compress the smallest amount vital bits of the encrypted image employing a data-hiding key to make a thin space to accommodate some additional data. With an encrypted image containing an additional data, if the receiver has data hiding key, he can extract the additional data though he does not know the image content. If the receiver has both the encryption key and the data hiding key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

An improved image secret writing formula supported chaotic system was planned by Shubo Liu, Jing Sun and Zhengquen Xu [6]. Chaos theory has been established since 1970's by many alternative analysis areas, like physics, arithmetic, engineering, and biology, etc. The distinct properties of chaos, like noise, quasi-randomness, sensitivity dependence on initial conditions and system parameters, have granted chaotic dynamics as a promising different for the traditional cryptographic algorithms. A brand new secret writing formula is planned by analyzing the principle of the chaos secret writing formula supported supply map. Moreover, the protection and performance of the planned formula is additionally calculable. The ciphertext generated by this methodology is that the same size because the plaintext and is appropriate for sensible use within the secure transmission of tip over the net. The foremost a part of the look could be a fresh planned chaos-based pseudo-random keystream generator (PRKG) supported one or two of chaotic systems.

Audio encryption using higher dimensional chaotic map was proposed by Gnanajeyaraman R, Prasadh and Dr. Ramar [7] explores the properties of chaotic maps have been widely used in audio encryption recently. In this paper, an analog audio input is sampled at frequency well above the nyquist frequency of the signal. Then an16 bit quantization is used to convert the analog signals into its equivalent decimal value by making these data with a random key stream generated by a chaos based pseudo random key stream generator, the corresponding encrypted audio is formed.

Hash basd data text fushion in speech signal using speech signal algorithm was proposed by Madhu, Anu Aggarwal and Anjali Sachdeva [8]. The term "fushion" generally literally means to embed something in some cover field. In this work, they hide text data using hash based functionality by finding the non area of interest(NAOI) in the speech signals. By using .wav file format for speech signals which is to be processed for fushion data into the image. Data is firstly converted into ASCII. The next task is to secure the data which is to be fused in to the voice signals that is done with the concept of HASHKEY, length of the hash key is totally based upon the data which we are going to hide under speech signal.

A novel algorithm for high-quality data embedding have been made in audio in [9]. It is based on changing the relative length of the middle segment between two successive maximum and minimum peaks to embed data. To ensure smooth monotonic behavior between peaks, a hybrid orthogonal and non orthogonal wavlet decomposition is used prior to data embedding.. This algorithm is invariant after time-scale modification, time shift and time cropping. It gives high-quality output and is robust to mp3 compression.

Spread–spectrum watermarking of audio signals is proposed by Darko Kirovski and Henrique S.Malvars in [10]. Watermarking has become a technology of choice for a broad range of multimedia copyright protection applications. In this system, the vector x is composed of magnitudes of several frames of a modulated complex lapped transform (MCLT) in a decibel (db) scale. The MCLT is a 2 x oversampled filter bank that provides perfect reconstruction. The MCLT is similar to a DFT filter bank, but it has

properties that makes it attractive for audio processing, especially when integrating with compression systems, because signals can easily be reconstructed from just the real part of the MCLT.

II. PREVIOUS ARTS

The previous methods used reversible data hiding (RDH) in encrypted images. There are many RDH techniques in encypted images and video such as difference expansion (DE), histogram shift method (HS), the state of art methods usually combined DE or HS method and least significant bit method (LSB).

A more popular method is based on difference expansion in which the difference of each pixel group is expanded. e.g., multiplied by 2 and thus the LSBs of the difference are all-zero and can be used for data embedding messages. Another promising strategy for RDH is histogram shift in which space is saved for data embedding by shifting the bins of histogram of grey values. The state of art methods usually combined DE or HS to residuals of the image, e.g., the predicted errors to achieve better performance. The above three methods are suited for encrypted images. LSB coding is the simplest way to embed information in an audio file. By substituting the least significant bit of each sampling point with a binary message, LSB allows for a large amount of data to be encoded.

This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. The information on the system is of some value to persons other than the sender and the intended receiver(s), e.g. personal, financial, intelligence or otherwise information that is sensitive in nature. Today competitors, hackers or governmental institutions can intercept any GSM cell call with relatively little effort. So in the above cases voice encryption systems are used to guarantee end-to-end security for speech in real time communication systems such as GSM, telephone, analogue radio. Similarly audio encryption is used for secret data communication in defense, research institute, medical information protection. By using reversible data hiding technique, we can enhance the protection system for secret data communication through data concealment in encrypted audio.

III. PROPOSED METHOD

The proposed method provides the enhancement of protection system for secret data communication through data concealment in encrypted audio. Data Embedding using pixel difference expansion and bit modification techniques have the drawbacks such as data hiding capacity low and more distortion due to hiding process, so it may degrade the image or audio quality. The data hiding technique uses the adaptive LSB replacement algorithm for concealing the secret message bits into the encrypted audio. It is chosen because the most common steganography method in audio and image files employs some type of least significant bit substitution or overwriting. The least significant bit term comes from the numeric significance of the bits in a byte. The high-order or most significant bit is the one with the highest arithmetic value (i.e., 2^7=128), whereas the low-order or least significant bit is the one with the lowest arithmetic value (i.e., 2^0=1).

Least significant bit substitution can be used to overwrite legitimate RGB color encodings or palette pointers in GIF and BMP files, coefficients in JPEG files, and pulse code modulation levels in audio files. By overwriting the least significant bit, the numeric value of the byte changes very little and is least likely to be detected by the human eye or ear.

The proposed encryption technique uses the chaotic algorithm to encrypt the audio and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After encryption, the data hider will conceal the secret data which is in encrypted form. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless.. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication.

The chaos encryption algorithm is used for audio encryption because the chaotic based cryptosystems are suitable for large-scale data encryption such as images, videos or audio. The experiments show that the algorithm has the characteristic of sensitive to initial condition, high key space,digital audio signal distribution uniformity and the algorithm will not break in chosen/known-plaintext attacks.

In the data extraction module, the secret data will be extracted by using relevant key for choosing the encrypted audio to extract the data. By using the decryption keys, the image and extracted text data will be extracted from encryption to get the original information. The main goal of this paper is to hide the text on audio. An audio file can be used as a host media to hide textual message without affecting the file structure and content of the audio file.The performance of PSNR is measured on proposed system. It computes the PSNR in decibel between two audios. PSNR is used as a quality measurement between the original and a compressed signal. The higher

the PSNR, the better the quality of the compressed or reconstructed audio.

3.1 Proposed Chaotic encryption Scheme

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation.Sensitive on initial stage and topology transitivity are the properties in it. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectorysectional value. Identical trajectory only can produce the same values. The topology transitivity defines that the state points reside in a bounded space state and approaches.

The chaos encryption method can facilitate to discover some essential information and establish the crucial stage of security. It is achieved by iterations. The properties of chaos are slightly producing some changes in the entire cryptography In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory.

Assume the initial conditions as the current route (trajectory). Iterate the chaotic equation until the path reaches the target site and then store the amount of iterations as a code for each message symbol. Encrypt the next message by iteration the recent trajectory produce the next cipher according to it and so on.

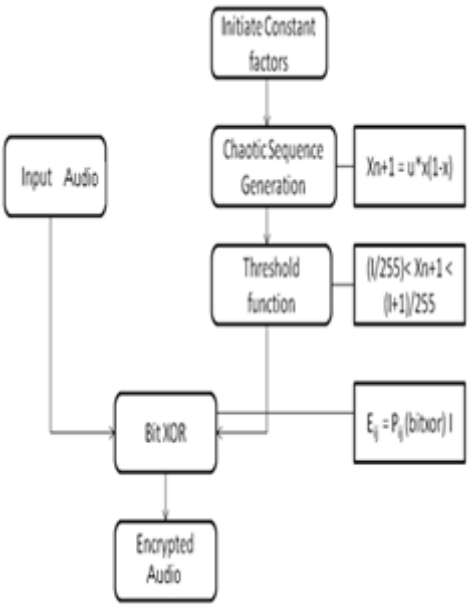

Fig.3.1.1 Proposed Chaotic Encryption Scheme.

3.2 Proposed RDH in encrypted audio file

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the

LSB method:

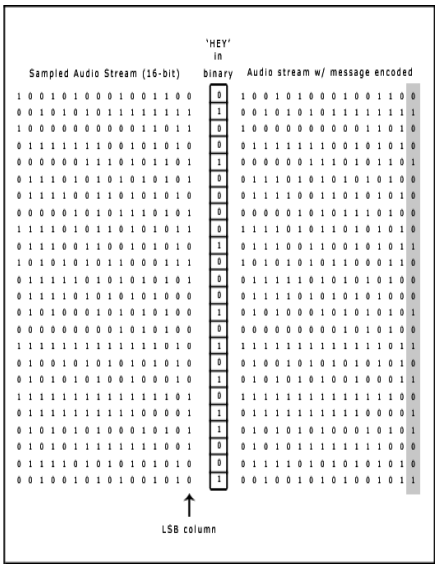

Fig. 3.2.1 Proposed LSB replacement technique

It performs bit level manipulation to inscribe the message. The subsequent steps are:

a. Receives the audio file in the shape of bytes and regenerate into bit pattern.

b. Every character within the message is regenerate in bit pattern.

c. Replaces the LSB bit from audio with LSB bit from character within the message.

In LSB coding, the ideal data transmission rate is 1Kbps per 1KHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in thea audio file as well. Thus one should consider the signal content before deciding on the LSB operation to use. The main advantage of of the LSB coding method is low computational complexity of the algorithm.

3.3 Proposed method results and analysis

The original audio file is converted into encrypted audio file. For data hiding in encrypted audio file, message has taken from the message text file. The message will be embedded into encrypted audio file. The embedded data were extracted from stego audio and original audio file is recovered.

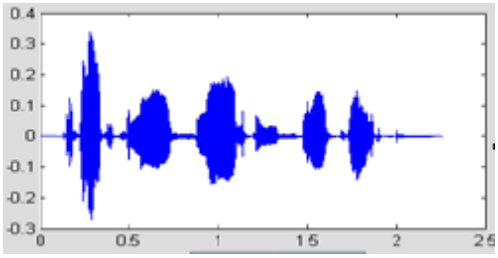

Fig 3.3 (a) Original audio file

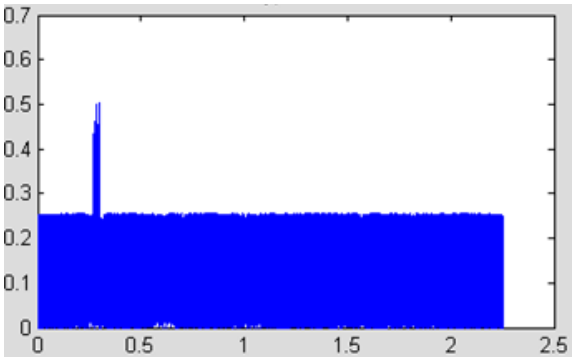

Fig. 3.3 (b) Proposed Encrypted Audio file

Data Embedded: Hello world

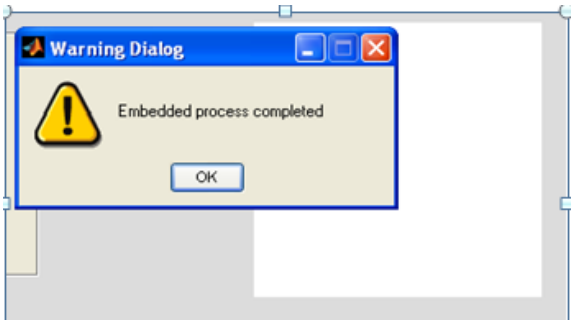

Fig. 3.3 (c) Proposed data embedding process in encrypted audio file

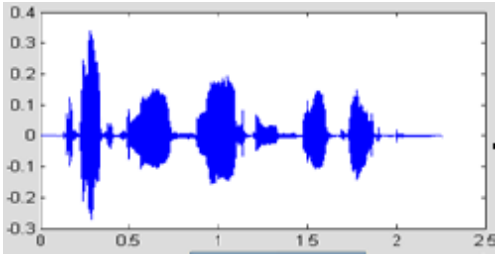

Fig. 3.3 (d) Decrypted audio file

IV. PERFORMANCE EVALUATION:

Comparision of performance evaluation for two different encrypted audio files with encrypted images is shown in the Table 4.1.

Table 4.1 Comparison of parameter analysis

Parameter	RDH in encrypted audio file 1	RDH in encrypted audio file 2	RDH in encrypted images
Percentage Residual difference(%)	0.9956	0.9781	-
Root mean square error(RMSE)	0.0015	0.0016	0.013123
Peak to signal noise ratio in dB	22.2011	25.5590	66.9506
Correlation coefficient	0.9999	1.0000	0.006287

V. CONCLUSION

This paper represents the protection of audio quality and hidden data during transmission based on approach of chaotic crypto system with LSB based data concealment. RDH technique is applied for data embedding in encrypted audio file for secret communication in the proposed system. Finally the performance of system was evaluated with quality metrics such as percentage residual difference, RMSE, PSNR and correlation coefficient are measured and compared with existing method of RDH in encrypted images. The proposed system is quite useful for applications in defence and medical information protection. It was better compatible approach and flexibility with better efficiency rather than prior methods. Instead of data embedding, image will be embedded into encrypted audio in future work for secret communication in the proposed system.

REFERENCES

[1]. T.Kalkerand M.Willems, "Capacity bounds and code constructions for Reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP 2002), 2002, pp. 71–76.

[2]. W.Zhang, B.Chen,and N.Yu "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS6958, 2011, pp. 255-269, Springer-Verlag.

[3]. J. Fridrich and M. Goljan,"Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Muktimedia Contents San Jose, CA, USA, Jan. 2002, vol. 4675, pp.572–583.

[4]. J.Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5]. X.Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf.

Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[6]. Shubo Liu, Jing Sun and ZhengquenXu, (2009) "An improved image encryption algorithm based on chaotic system," Journal of computers vol.4,no.11.

[7]. R.Gnanajeyaraman, K.Prasadh and Dr.Ramar, " Audio encryption using higher dimensional chaotic map," Int..journal of recent trends in engineering vol.1,no.2. 2009

[8]. Madhu, Anu Aggarwal and Anjali Sachdeva, "Hash based data text Fushion in speed signal using speech signal algorithm," Int. journal of computing & business research, 2012.

[9]. Mohamed F.Mansour and Ahmed H.Tewfik, "Time scale invariant audio data embedding," EURASIP journal on applied signal processing ,993-1000, 2003.

[10]. Darko Kirovski and Henrique S.Malvar, "Spread spectrum watermarking of audio signals," IEEE transactions on signal processing, vol. 51, no.4, 2003.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Dr.M.Kavitha. "An Modified Enhanced Method of Reversible Data Hiding In Audio Encryption." International Journal of Engineering Research and Applications (IJERA), vol. 7, no. 8, 2017, pp. 28–33.