Available online at www.sciencedirect.com

SciVerse ScienceDirect

AASRI Procedia 1 (2012) 498 – 504

AASRI Procedia

www.elsevier.com/locate/procedia

2012 AASRI Conference on Computational Intelligence and Bioinformatics

Applied Research in Communications Encryption Technology Based on the Integration of Digital Watermarking

Li Qiuyan[a*] , Du Chunmei[b] , Meng Qinghua[a], Zhang Lei[b] , Gao Wenju[a]

[a]*Changchun Institute of Engineering Technology, Changchun, 130117, China*
[b]*Air Force Aviation University China, Changchun, 130022 , China*

Abstract

This essay describes a new radio encryption technique among communication equipments, that is embed confidential information in normal carrier by using digital watermarking to achieve the purpose of protecting confidential information and confusing illegal interceptors. Meanwhile it also gives embed watermarking based on integration and Detection Algorithm.

Keywords: Digital Watermarking, Covert Communications, Content Authentication, Carrier, Robustness, vulnerability, integration.

1. Introduction

Communication equipment radio, especially military radios, which wish only the receiver receives communication contents, namely to ensure the communication information is confidential. The traditional approach is by using encryption technique of cryptology to encrypt communication content; as a result, other receivers without secret key cannot understand the contents. As information become mojibake after being encrypted, it is easy to attract interceptors' attention and arouse their desire of password cracking. Once the content is decrypted there is no longer a protective action; even if the interceptor cannot crack, he also can intercept the confidential information successfully or can interfere with the procedure of communication. Therefore, cryptology can only protect the contents in transferring.

* *E-mail address:* lili000643@sohu.com

doi:10.1016/j.aasri.2012.06.078

Therefore, it is in urgently need of another kind of alternative technology or technology replenishing cryptology, which should even be able to continue to protect content after it is decrypted. The "digital watermarking" of covert communication technology has the capacity to meet these requirements, because it not only protects the content of the communicating information, but more important it hides the existence of communication facts, and thus confuse interceptors. After confidential information is encrypted, and then conduct covert communication, which adds another layer of protection. Meanwhile in general use digital watermarking will not be eliminated. Even after the process of decryption, encryption, compression, digital - analog conversion and the file format transformation, the clever designed watermark can continue to exist.

The biggest advantage of covert communication is that except for the two sides of communication, any other third parties don't know the existence of covert communication, which is more protective than simply encrypt code, making the encryption mechanism from "cannot understand" to "invisible" to avoid being the attack target for busybodies.

For example, hide confidential information (images, texts, and sounds) in the public image, and then transmit, which looks like other non-confidential images, with the result of being very easy to escape the attention or password-cracking of the illegal interception. This is what the traditional encryption communication system lack of; it is in this case that makes the hidden communication technology has important application prospect in military communications.

2. Concept of digital watermarking and system model

The so-called Digital Watermarking technology refers to embed covert information in digitized data like voice, image or video, these information is usually invisible and cannot be observed or aware of by human vision perceptual system, can only be collected by dedicated monitor or reader.[3] Through information which hided in the multi-media contents, people can reach the purpose of confirming contents creator, purchaser or judging whether the contents are true, complete or not.

Digital watermarking is an important branch of information hiding technology research. By embedding confidential information ——watermarking in original data, it affirms the ownership of the data, verifies integrity of data, tracks the source of data, controls usage of data and delivery of confidential information. According to goal and requirement of covert information, digital watermarking should have the following basic characteristics:

- Hide: watermark information and source data integrate together, without changing the data storage space; besides the source data must not has obvious change phenomenon.
- Robustness: It means that embedded watermarking data after going through various processing operation and against operation, which avoid losing or damage the watermarking information.
- Security: it refers the now location and content of watermarking information is unknown, which needs to apply covert arithmetic and take measures like adopting pretreatment (for example, encryption) to watermarking.

All digital watermarking systems compose two essential parts: watermarking embedding system and watermarking detection system. Fig. 1 and Fig. 2 respectively represent the general process of watermarking embedment and watermarking detection:

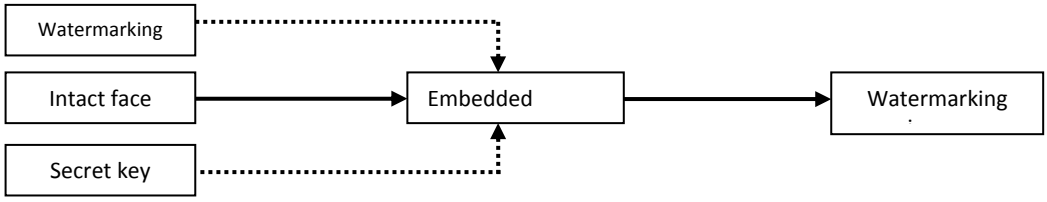

Fig. 1. watermark embedding process

In the process of watermarking embedment, the first step is t produce watermarking. The information you want to embed in can be all kinds of nature, such as number, image and text so forth. The use of password is to enhance the security by protecting non-authorized people from reading messages. The output of watermarking embedding process is image works with embedded watermarking.

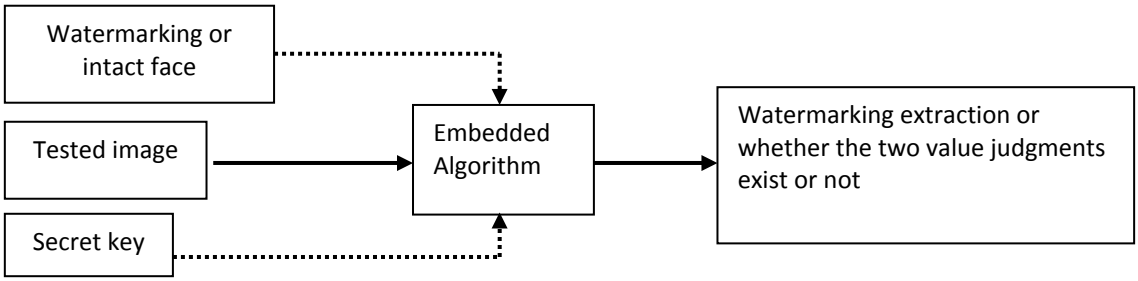

Fig. 2. watermarking detection processes

The input of the watermarking detection process is the image be tested, it may not be watermarking embedded, or it may be images been watermarking embedded and then attacked. Because of different watermarking algorithm, the input of watermarking detection process can also be password, intact face and so on. The Input of the watermarking detection process may be the watermarking been detected, or a confidence value about whether watermarking is involved in the detected signals.

When the radios transfer confidential information, they embed confidential information as watermarking in a carrier which can be put in public. The carrier can be digital signals like text, picture and sound.

In radio watermarking encryption scheme, it should use double or multiple watermarking mechanism: in carriers except for embedding robustness watermarking in order to hide information, it also embeds half fragile watermarking unrelated to contents, fragile watermarking, in the use of distinguishing from enemy and recognizing if the information are attacked or distorted. Once we can't detect the watermarking, we can judge the original contents are attacked or they are not from our party, which can be effectively prevent statistical attack which robustness watermarking can't resist.

3. watermarking algorithm based on integration

One important application of digital watermarking is data hiding. In the approved watermarking project, it just needs to judge whether the watermarking exist or not, so meaningless watermarking can be embedded. However, in the watermarking project carrying with confidential data, the watermarking is meaningful and the amount of information of watermarking is bigger.

Technology methods of data hidden mainly have spatial domain algorithm and transform domain algorithm. Digital image hiding algorithm based on integration is one kind of spatial domain algorithm. It uses Bzier Curve one time, hiding confidential images in the original images which have the same size. This kind of algorithm has the characteristics of simple calculation, easy to realize and high quality of regained confidential image. It also can embed any form of binary stream files in digital images. In selecting proper parameters, it can exactly recover the binary stream files. The biggest feature of this algorithm is high ability of hiding data. In the case of gray level image the same as original image, its biggest hidden ability can be 3bits / pixel, so the main application of this algorithm is hide of confidential data.

3.1. Basic idea based on integration

In Computer Graphics and Computer aided design, we often use a kind of blending function method, that is suppose we preset n+1 point in the space, then P_0,P_1, to P_n call parametric curve below the n times Bzier Curve, whose control point is {P\i=1,1,…,n}.

$$p(t)=\sum_{i=0}^{n}P_i B_i^{\ n}(t) \tag{1}$$

Hereinto $B_i^{\ n}(t)$ is the primary function of Berntein

$$B_i^{\ n}(t)=\begin{bmatrix} n \\ i \end{bmatrix}(1-t)^{n-i}t^i \tag{2}$$

Normally we treat broken line P_0,P_1, to Pn as Control Polygon of P(t), point P_0,P_1, to P_n as Control vertex of P(t).

In the following essay, 1 time Bzier Curve will be exemplied to disscuss the integration of these two digital images.

From (1)、(2), we can deduce

$$P(t)=(1-t)P_0+tP_1 \tag{3}$$

It is a simple linear interpolation formula.

As for original image F_0 and F_1, suppose their sizes are both $M\times N$, then we can have

$$F_0=\{f_{ij}^{\ 0},0\le f_{ij}^{\ 0}\le 255,0\le i<M,0\le j<N\}$$

and

$$F_1=\{f_{ij}^{\ 1},0\le f_{ij}^{\ 1}\le 255,0\le i<M,0\le j<N\}$$

as to applying formula (3) of each pair of pixel $f_{ij}^{\ 0}$ and $f_{ij}^{\ 1}$ of the same position in F_0 and F_1, we have

$$f_{ij}^{\ 2}=\left\lfloor (1-t)^{f_{ij}^0}+t^{f_{ij}^1}\right\rfloor 0\le i<M,0\le j<N \tag{4}$$

Then we deduce fusion image, hereinto $\lfloor X\rfloor$ refers to the MaxInt which is smaller than or equals to X.

Through formula (5)and (6), we can regain original images and confidential images from fusion image.

$$f_{ij}^{0}=\left\lfloor \frac{f_{ij}^{\ 2}-tf_{ij}^{\ 1}}{1-t}\right\rfloor,0\le i<M,0\le j<N \tag{5}$$

$$f_{ij}^{1}=\left\lfloor \frac{f_{ij}^{\ 2}-(1-t)f_{ij}^{\ 0}}{1-t}\right\rfloor,0\le i<M,0\le j<N \tag{6}$$

Apply (6) in the picture, we will gain images been recovered.

3.2. Watermarking algorithm based on integration

3.2.1 Construct confidential images

This algorithm can embed any form of data files which is input by bit stream. Define String Length L,

resolve bit stream into substring whose length is L, in accordance with orders from up to down, left to right, rank substring into matrix $S_{M\times N}=\begin{bmatrix} S_{11} & S_{12} & \dots & S_{1N} \\ S_{M1} & S_{M2} & \dots & S_{MN} \end{bmatrix}$ in the ize of M×N, hereinto, S_{ij} is bit substring long for L. Note: here confine total length of bit stream is not longer than M×N×L, inadequate part add 0 to make element t_{ij} in matrix $T_{M\times N}$ whose size is M×N equal to bit substring decimal in the same position of matrix $S_{M\times N}$, that is $T_{M\times N}=\begin{bmatrix} t_{11} & t_{12} & \dots & t_{1N} \\ t_{M1} & t_{M2} & \dots & t_{MN} \end{bmatrix}$, here $(t_{ij})_{10}=(S_{ij})_2$, at present the numeric area of element in matrix $T_{M\times N}$ is [0，2^L-1]. In order to make the constructed secret image F_1's pixel value is between [0，255], command $f_{ij}^{\ 1}=t_{ij}\times 2^{8-L}$, now the short-cut process of pixel value $f_{ij}^{\ 1}$ of confidential image F_1 is $\{f_{ij}^{\ 1}\,|\,f_{ij}^{\ 1}=i\times 2^{8-L}, i\in[0,2^L-1]\}$ | .

3.2.2 Embedded Algorithm

Take advantage of digital image hiding technology thoughts based on integration to embedded data. As to original image F_0 and F_1, suppose their sizes are both M×N, then

$$F_0=\{f_{ij}^{\ 0},0\le f_{ij}^{\ 0}\le 255,0\le i<M,0\le j<N\}$$

and

$$F_1=\{f_{ij}^{\ 1},0\le f_{ij}^{\ 1}\le 255,0\le i<M,0\le j<N\}$$

To reduce error caused by data embedding and recovering, amend formula (4), apply formula (7) in each pair of pixel $f_{ij}^{\ 0}$ and $f_{ij}^{\ 1}$ in the same position of F_0 and F_1,

$$f_{ij}^{\ 2}=round\left(f_{ij}^{\ 0}\times(1-t)\right)+round\left(f_{ij}^{\ 1}\times t\right) \tag{7}$$

we get: $F_2=\{f_{ij}^{\ 2},0\le f_{ij}^{\ 2}\le 255,0\le i<M,0\le j<N\}$, here round(x) refers to the nearest integer from X.

3.2.3 Abstract algorithm

The process of restoring confidential information from fusion image is the inverse process of embedding data. First of all, restore confidential image from fusion image, the method is as follows:

$$f_{ij}^{\ 1}=round\left(\left(f_{ij}^{\ 2}-round\left((1-t)\times f_{ij}^{\ 0}\right)\right)/t\right) \tag{8}$$

Then we get confidential imager $F_1=\{rf_{ij}^{\ 1},0\le rf_{ij}^{\ 1}\le 255,\ 0\le i<M,\ 0\le j<N\}$

Before we abstract confidential information from confidential images, we have to amend errors exist in confidential images, the process is as follows:

$$rf_{ij}^{1}=\begin{cases} rf_{ij}^{\ 1}, & rf_{ij}^{\ 1}\bmod 2^{8-L}\le 2^{8-L-1} \\ rf_{ij}^{\ 1}+2^{8-L-1}-1, & Otherwise \end{cases} \tag{9}$$

The numeric area of the amended pixel value r $f_{ij}^{\ 1}$ is still [0，255], at last we can abstract bit higher L to

get rs_{ij} from the amended pixel value rf_{ij}^{1},

$$\left(rs_{ij}\right)_2 = \left(rt_{ij}\right)_{10} = \left\lfloor rf_{ij}^{1} / 2^{8-l} \right\rfloor \tag{16}$$

Then in accordance with the inverse process of constructing confidential images, we can get the bit stream embedded.

3.3. experimental data

As to original image, according to formula (7) we know that its peak Signal Noise Ratio is

$$PSNR = 10\lg\left[\frac{M\times N\times 255}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f_{ij}^{2}-f_{ij}^{0})^2}\right] \approx 10\lg\left[\frac{M\times N\times 255}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(t(f_{ij}^{0}-f_{ij}^{1}))^2}\right] \geq 20\lg\left[\frac{1}{t}\right] \tag{17}$$

According to the empirical value requirements for PSNR, it shall has

$$20\lg\left[\frac{1}{t}\right] \geq 28 \tag{18}$$

From formula （18）, we know

$$t \leq 0.03981\text{。} \tag{19}$$

As it is only when 0.5/t+0.5≤28-L-1-1 can we correctly restore confidential information. From condition “0.5/t+0.5≤28-L-1-1”and formula (19), we can find out numeric area of string length L:

$$L \leq 3.1926 \tag{20}$$

And because L is the length of bit substring, it can only be positive integer. So L is [1，2，3].Chart 1 finds out when L takes different value, the numeric area of t and the biggest hide ability when 8bits / pixel gray level image is the original image.

Chart 1 the numeric area of t and the biggest embedded ability when L is in different value

	L=1	L=2	L=3
the numeric area of t	[0.008,0.03981]	[0.01639,0.03981]	[0.03448,0.03981]
the biggest hide ability	1bit/pixel	2 bit/pixel	3 bit/pixel

4. Conclusion

The development of digital watermarking technology just has ten years, Data hiding by the use of digital media is still a new field of study, but it also is a practical which is closer combined with specific application. The realization of encrypting radio confidential information by using digital watermarking technology is also a new try. The results will be better if it is combined with the existing encryption technology. We believe there will be new radio security equipments made by digital watermarking in the future.

References

[1]Deng Zhenhua, Yao Youwen "information hiding technology development and application, the Defense

Information, 2004 37 ~ 39
[2]Boxiao Chen, Shen Lin, often Vincent, digital watermarking technology: concepts, applications, and the status quo ", Computer World, 2000, 1 to 4 page.
[3]Su Yuk Ting Zhang Chuntian in disguise covert communications technology, "Communications Technology in September 1998 3 35-37