Journal of Artificial Intelligence
ISSN: 2229-3965 & E-ISSN: 2229-3973, Volume 3, Issue 2, 2012, pp.-94-97.
Available online at http://www.bioinfo.in/contents.php?id=71

STEGANOGRAPHY ALGORITHM WITH DYNAMIC PATTERN MATCHING

YOGADHAR PANDEY AND JAGDISH PIMPLE*

Department of Computer Science & Engineering,SIRT Bhopal, MP, India.
*Corresponding Author: Email- pimplejagdish@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- The access and distribution of digital information revolution has brought about profound changes in our society and our lives. Because of many advantages of digital information, generate new challenges and new opportunities for innovation. The issue is regarding multimedia data hiding, its application to multimedia security and communication, which address both the theoretical and practical aspects, and tackle both design and attack problems.
Data hiding is modeled to handle communication problem where the embedded data has to be transmitted. Various embedding mechanisms are provided with different robustness-capacity. This mechanism has two major categories of embedding data. In addition, it is observed that the unevenly distributed embedding capacity brings difficulty in data hiding. Thus a comprehensive solution to this problem is, addressing the considerations for choosing constant or variable embedding rate and enhancing the performance for each case.This paper presents a Steganography method using lossy compressed video which provides a natural way to send a large amount of secret data. The proposed method is based on wavelet compression for video data and bit-plane complexity segmentation (DYNAMIC PATTERN) Steganography. In wavelet-based video compression methods such as 3-D set partitioning in hierarchical trees (SPIHT) algorithm and motion-JPEG2000, wavelet coefficients in discrete wavelet transformed video are quantized into a bit-plane structure and therefore DYNAMIC PATTERN Steganography can be applied in the wavelet domain.3-D SPIHT-DYNAMIC,PATTERN. Steganography and motion-JPEG2000-DYNAMIC PATTERN Steganography are presented and tested, which are the integration of 3-D SPIHT video coding and DYNAMIC PATTERN Steganography and that of motion-JPEG2000 and DYNAMIC PATTERN, respectively. Experimental results show that 3-D SPIHT-DYNAMIC PATTERN is superior to motion-JPEG2000-DYNAMIC PATTERN with regard to embedding performance.
Keywords- Steganography, SPIHT, DPIS, BPCS, DWT, Dynamic pattern.

Citation: Yogadhar Pandey and Jagdish Pimple (2012) Steganography Algorithm With Dynamic Pattern Matching. Journal of Artificial Intelligence, ISSN: 2229-3965 & E-ISSN: 2229-3973, Volume 3, Issue 2, pp.-94-97.

Introduction

Steganography is the practice of hiding a secret data in an innocent looking dummy container. This container may be a digital still image, audio file, video file, or even a printed image. Once the data has been embedded, it may be transferred across insecure lines or posted in public places. Therefore, the dummy container should seem innocent under most examinations. In previous Steganography algorithms, bit-plane decomposition was commonly used combined with the simple approach of replacing the binary data in the least significant bit-planes of a dummy image with secret binary data. We previously presented a sophisticated stenography method, called bit-plane complexity segmentation (DYNAMIC PATTERN) Steganography, which makes use of bit-plane decomposition and the characteristics of the human vision system. Noting that human cannot perceive(to aware of) any shape information in a very complicated binary pattern, we can replace noise-like regions in the bit-planes of the dummy image with secret data without deteriorating the image quality.

This project presents a Steganography method using lossy compressed video which provides a natural way to send a large amount of secret data. The proposed method is based on wavelet compression for video data and DYNAMIC PATTERN Steganography. In wavelet-based video compression methods such as three-dimensional (3-D) set partitioning in hierarchical trees (SPIHT) algorithm and Motion-JPEG2000, wavelet coefficients of video by discrete wavelet transform (DWT) are quantized into a bit -plane structure and therefore DYNAMIC PATTERN steganography can be applied in the wavelet domain. In this project, 3-D SPIHT-DYNAMIC PATTERN steganography and Motion-JPEG2000-DYNAMIC PATTERN steganography are presented, which are the integration of 3-D SPIHT video coding and DYNAMIC PATTERN steganography, and that of Motion-JPEG2000 and DYNAMIC PATTERN, respectively.Internet communication has become an integral part of the Infrastructure of today's world. The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication be done in secrete. Such secret communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. With email, many people wrongly assume that their communication is safe because it is just a small piece of an enormous amount of data being sent worldwide. After all, who is going to see it? But in reality, the Internet is not a secure medium, and there are programs "out there" which just sit and watch messages go by for interesting information.

Encryption provides an obvious approach to information security, and encryption programs are readily available. However, encryption clearly marks a message as containing "interesting" information, and the encrypted message becomes subject to attack. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent secret information.

Some of them use the least significant bits of the image data to hide the data. Other programs embed the secret information in a Steganography presents another approach to information security. In steganography, data is hidden inside a vessel or container that looks like it contains only something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files.

In recent years, several steganographic programs have been posted on Internet home pages. Most of them use image data for the container of the specific band of the spatial frequency component of the carrier Some other programs make use of the sampling error in image digitization. However, all those steganography techniques are limited in terms of information hiding capacity. They can embed only 5-15 % of the vessel image at the best. Therefore, current steganography is more oriented to water marking of computer data than to secret person-person communication applications. We have invented a new technique to hide secret information in a color image. This is not based on a programming technique, but is based on the property of human vision system. Its information hiding capacity can be as large as 50% of the original image data. This could open new Applications for steganography leading to a more secure Internet Communication age.

Digital images are categorized as either binary (black-and-white) or multi-valued pictures despite their actual color. We can decompose an n-bit image into a set of n binary images by bit-slicing operations . Therefore, binary image analysis is essential to all digital image processing. Bit slicing is not necessarily the best in the Pure-Binary Coding system (PBC), but in some cases the Canonical Gray Coding system (CGC) is much better .

BPCS Steganography

Bit-Plane Complexity Segmentation Steganography is our new steganographic technique, which has a large information hiding capacity. As was shown in the previous section, the replacement of the complex regions in each bit-plane of a color image with random binary patterns is invisible to the human eye. We can use this property for our information hiding (embedding) strategy. Our practical method is as follows.

In our method we call a carrier image a "vessel" or" dummy" image. It is a color image in BMP file format, which hides (or, embeds) the secret information (files in any format). We segment each secret file to be embedded into a series of blocks having 8 bytes of data each.

These blocks are regarded as 8 X8 image patterns. We call such blocks the secret blocks. We embed these secret blocks into the vessel image using the following steps.

Algorithm

1. Transform the dummy image from PBC to CGC system.
2. Segment each bit-plane of the dummy image into informative and noise-like regions by using a threshold value (a0). A typical value is a0 = 0.3.
3. Group the bytes of the secret file into a series of secret blocks.
4. If a block (S) is less complex than the threshold(a0) , then Conjugate it to make it a more complex block (S*). The conjugated block Must be more complex than (a0).
5. Embedded each secret block into the noise-like regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks). If the block is conjugated, then record this fact in a "conjugation map."
6. Also embed the conjugation map as was done with the secret blocks
7. Convert the embedded dummy image from CGC back to PBC.

The Decoding algorithm (i.e., the extracting operation of the secret information from an embedded dummy image) is just the reverse procedure of the embedding steps.

The novelty in DYNAMIC PATTERN-Stenography is itemized in the following.

A. Segmentation of each bit-plane of a color image into "Informative" and "Noise-like" regions.
B. Introduction of the B-W boarder based complexity measure for region segmentation
C. Introduction of the conjugation operation to convert simple secret blocks to complex blocks.
D. Using CGC image plane instead of PBC plane

DYNAMIC PATTERN-Stenography

Visual cryptography provides a friendly environment to deal with images. Generally cryptography tools supports only one kind of image formats. Our application supports .gif and .png (portable network graphics) formatted images and our application has been developed using swing and applet technologies, hence provides a

friendly environment to users.

- In Steganography, data is hidden inside a vessel or container that looks like it contains only something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files.
- All of the traditional steganographic techniques have limited information-hiding capacity. They can hide only 10% (or less) of the data amounts of the vessel.
- This Technique uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel.
- We can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality.
- We termed our Steganography "DYNAMIC PATTERN-Stenography," which stands for Bit-Plane Complexity Segmentation Stenography.

3-D SPIHT (set partitioning in hierarchical trees) algorithm was proposed for video compression by extending 2-D SPIHT algorithm for image compression. 3-D SPIHT has the following characteristics:

partial ordering by magnitude of 3-D wavelet transformed video,

ordered bit-plane coding, and

The successive approximation method used by 3-D SPIHT algorithm encodes wavelet coefficients one bit-plane at a time, starting with the most significant bit. In 3-D SPIHT compression, each wavelet coefficient w is expressed as

$$w = T(a_0 + a_1 2^{-1} + \cdots + a_{n-1} 2^{-n+1}),\ \ a_i \in \{0,1\},$$

where T = 2[log2 wmax] (wmax is the maximum absolute value among all wavelet coefficients in a 3-D DWT video).Since (a0 + a12−1 + · · ·+an−12−n+1) is a binary expression, the 3-D DWT video can be considered to have a bit plane structure and therefore DYNAMIC PATTERN Steganography can be applied in the wavelet domain. The wavelet coefficients have many image-like properties, and DYNAMIC PATTERN Steganography is ideal for exploiting them.

The main properties leveraged for DYNAMIC PATTERN Steganography are:

1. Correspondence: Spatial areas in each section of the sub bands correspond directly to areas in the original image.
2. Complexity: The bit-planes at corresponding significance levels of the wavelet coefficients and the original image are usually proportionally complex.
3. Resilience: Changes in the values of the wavelet coefficients do not create disproportionately large changes in the reconstructed image.

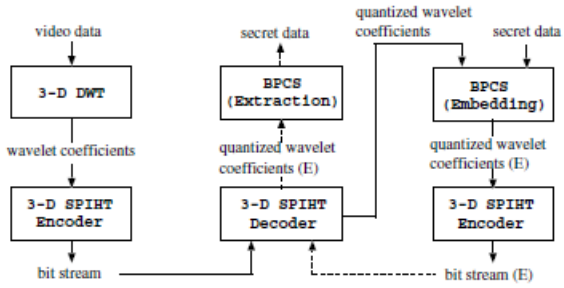

Fig. 1- A flowchart of data embedding and extraction in 3-D SPIHT-BPCS steganography

The procedure for data embedding and extraction in 3- D SPIHT-DYNAMIC PATTERN Steganography is shown in Fig. 1. The entire process to embed data in 3-D SPIHT-DYNAMIC PATTERN stenography follows the solid line arrows in Fig. 1. After 3-D DWT is applied to an original video, 3-D SPIHT encoder is applied to the wavelet coefficients and a bit-stream (compressed video file) is produced. Then the bit-stream is decoded by 3-D SPIHT decoder and quantized wavelet coefficients are derived1. Using these quantized wavelet coefficients, bit-planes for the wavelet coefficients can be constructed and used to embed secret data by DYNAMIC PATTERN Steganography (See the upper box of the right part in Fig. 1).The quantized wavelet coefficients modified by embedding are then subjected to 3-D SPIHT encoding again to produce a secret-data-embedded bit-stream. The mark (E) in Fig. 1 depicts that secret data is embedded. Data embedding in an already compressed video file is also possible. In this case, the process starts with a compressed video file, i.e., a bit-stream from the bottom of the middle part in Fig. 1 and follows the same process as the aforementioned one. The data extraction procedure follows the dashed arrows in Fig. 1. 3-D SPIHT decoding of secret -data-embedded bit-stream produces secret-data-embedded quantized wavelet coefficients. Extraction of secret data is carried out by the DYNAMIC PATTERN method using the quantized wavelet coefficients. We assume that the data extraction starts after the entire file of the bit-stream has been received.

Expected Outcome

Bit-Plane Complexity Segmentation Steganography is our new steganographic technique, which has a large information hiding capacity. As was shown in the previous section, the replacement of the complex regions in each bit-plane of a color image with random binary patterns is invisible to the human eye. We can use this property for our information hiding (embedding) strategy. Our practical method is as follows.

In this method we call a carrier image a "vessel" or" dummy" image. It is a color image in BMP file format, which hides (or, embeds) the secret information (files in any format). We segment each secret file to be embedded into a series of blocks having 8 bytes of data each.

These blocks are regarded as 8X8 image patterns. We call such blocks the secret blocks. We embed these secret blocks into the vessel image.

It shows the original image, Stegano image and modified pixels in the Stegano image of various samples taken. By observing the Stegano image, it is clear that the visual quality generated by secure authentication Steganography for binary images using pattern matching data hiding scheme is very good.

Fig. 5.1a- Fig. 5.1b- Fig. 5.1c-

Fig 5.5- a) Original copy (b) Marked copy with 89-Bytes embedded in (c) Difference between original and marked image

Distortion Measure

Two of the metrics used to compare the marked image and the

original image are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). The MSE is the cumulative squared error between the compressed and the original image, whereas PSNR is a measure of the peak error. It uses a standard mathematical model to measure an objective difference between two images. The mathematical formulae for the two are,

$$\text{MSE}= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \frac{(I(x,y) - I'(x,y))2}{M \times N}$$

$$\text{PSNR}= 20 \times \log 10 \frac{255}{sqrt(MSE)},$$

Where I(x, y) is the original host image and I'(x, y) is the watermarked image and M,N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the modified pixels in watermarked image. So, if a data embedding scheme having a lower MSE (and a high PSNR), it is recognized as a better one.

The PSNR and MSE obtained for the Pic78 Image size in bits 600 X 480, Total no. of M X N 864054, no. of ready block 734, on. Of pixels modified 3712, PSNR in db 38.2539, MSE 0.0014.

Table 5.1- Encoding and Decoding Timing & PSNR value

Host Image	Secret Image	Timing for Encoding	Timing for Decoding	PSNR value
Pic78	Pic78Word	20.8906s	15.4 s	38.253 dB
Pic2	Pic2jpg	11.65 s	9.09 s	38.091 dB
Pic38	Pic38exe	21.56 s	17.6 s	37.910 dB
Pic98	Pic98bmp	14.46 s	9.8 s	38.100 dB

Conclusions

Steganography is the art and science of communicating in a way which hides the existence of The communication. In contrast to cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present.

The security of data is of extreme importance in today's information-based society, including the fields of military, diplomacy, corporation, medicine, and even the individual, the information have to be safeguarded to avoid the unauthorized or illegal accesses and prevent the misuses and abuses.Any system, method or technique that deal with, processing information (data), and put this data in shapes or forms of media under the condition that it must be not visible in its new form for human observer. All such systems are called hiding systems for information.

The objective of this paper was to demonstrate our DYNAMIC PATTERN-Steganography, which is based on a property of the human visual system. The most important point for this technique is that humans cannot see any information in the bit-planes of a color image if it is very complex. We have discussed the following points and showed our experiments.

1. We can categorize the bit-planes of a natural image as informative areas and noise-like areas by the complexity thresholding.
2. Humans see informative information only in a very simple binary pattern.
3. We can replace complex regions with secret information in the bit-planes of a natural image without changing the image quality. This leads to our DYNAMIC PATTERN-Steganography.
4. Gray coding provides a better means of identifying which regions of the higher bit planes can be embedded.
5. A DYNAMIC PATTERN-Stenography program can be customized for each user. Thus it guarantees secret Internet communication. We are very convinced that this stenography is a very strong information security technique, especially when combined with encrypted embedded data.

References

[1] Feng Liu and Chuankun Wu (2011) *IEEE Transactions on information forensics and security*, 6(2).

[2] Raja K.B., Kiran Kumar K., Satish Kumar N., Lashmi M.S., Preeti H., Venugopal K.R. and Patnaik L.M. (2007) *International Conference onInformation System Security* 4812, 51-63.

[3] Fard A.M., Akbarzadeh M.R. and Varasteh A.F. (2006) *International Conference on Engineering of Intelligence Systems*, 1 -6.

[4] ElShafie D.R., Kharma N., Ward R. *International Symposium on Communications, Control and signal Processing*, 1263-1267.

[5] Chen P., Lin H. (2006) *International Journal of Applied Science and Engineering*, 4(3), 275-290.

[6] Lai B. and Chang L. (2006) *Lecture Notes in Computer Science*, 4319.

[7] Katzenbeisser S. and Petitcolas F.A.P. (2000) *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House.

[8] Niimi M., Noda H. and Kawaguchi E. (1998) *Trans. of IEICE*, J81-D-II, 1132-1140.

[9] Kawaguchi E. and Eason R.O. (1998) *SPIE*, 3528, .464-473.

[10] Spaulding J., Noda H., Shirazi M.N. and Kawaguchi E. (2002) *Pattern Recognition Letters*, 23, 1579-1587.

[11] Noda H., Spaulding J., Shirazi M.N., Niimi M. and Kawaguchi E. (2003) *Lecture Notes in Computer Science*, 2578, 295-309.

[12] Abdullah M.A.A. Ja'far (2003) *Informatics Institute for Postgraduate Studies*, M.Sc. thesis, Baghdad, Iraq.

[13] Johnson N.F., Duric Z. and Jajodia S. (2001) *Information Hiding: steganography and Watermarking Attacks and Countermeasures*, Kluwer a Cadmic Publishers, Boston, USA.

[14] Katzenbeisser S. and Petitcolas F.A.P. (2000) *Information Hiding Techniques for Steganography and digital watermarking*, Artech House, INC., Norwood, London.