A Layered Approach for Watermarking In Images Based On Huffman Coding

D. Lalitha Bhaskari[1] P. S. Avadhani [1] M. Viswanath[2]

[1] Department of Computer Science & Systems Engineering, Andhra University,
[2] Research Assistant, Department of Computer Science & Systems Engineering, Andhra University,
Visakhapatnam, Andhra Pradesh, INDIA

ABSTRACT: With the rapid increase of the internet users and the bandwidth is appreciable but at the same also brought some problems beside its advantages. The great facility in copying a digital content rapidly, perfectly and without limitations on the number of copies has resulted the problem of copyright protection. The ease with which duplication of digital information can be done has raised the need for us to take care of copyright and copyright protection mechanisms. One way to protect digital data against illegal recording or retransmission is to embed a signal, amount of data called a digital signature or copyright label or watermark that completely provides with the authentication or ownership of the user. In this work we propose a new algorithm through which we can embed more data than the regular methods under spatial domain. We compress the secret data using Huffman coding and then this compressed data is embedded using modified auxiliary carry watermark method. In this method our main contribution is towards increasing the amount of information which is to be embedded and at the same time increasing the security of the algorithm also.

Key words: Modified Auxiliary carry method, Huffman coding.

1. Introduction:

With the increasing use of e- media and the technology, transmission of high quality images, documents, video and audio has considerably increased. However, the availability of inexpensive hardware (such as printers, scanners, and compact disc and digital versatile disc burners), and powerful software is making unauthorized copying easy which is a major set back to the music, film, book and software publishing industries. Thus there is an increasing need for software or hardware that allows for protection of ownership rights, and it is in this context where watermarking techniques come to our help. Digital representation of signals brings many advantages when compared to analog representations, such as lossless recording and copying, convenient distribution over networks, easy editing and modification, and durable, cheaper, easily searchable archival. Unfortunately, these advantages also present serious problems including wide spread copyright violation, illegal copying and distribution, problematic authentication, and easy forging. Piracy of digital photographs is already a common phenomenon on the Internet. Today, digital photographs or videos cannot be used in the chain of custody as evidence in the court because of nonexistence of a reliable mechanism for authenticating digital images or tamper detection. Data hiding in digital documents provides a means for overcoming those problems. Digital watermarking are some of the techniques which are playing a significant role in the field of security. Cryptography is probably the most common method of protecting digital content. The content is encrypted prior to delivery, and a decryption key is provided only for legitimate copies of the content. Cryptography can protect the content in transit, but once decrypted, the content has no further protection. N Cryptography anybody can see that both the parties are communicating in secret Information hiding, Steganography, watermarking techniques has the potential to fulfill this need [3]. These three fields have a great deal of overlap and share many technical approaches. Information hiding is a general term which refers to keeping the existence of the information secret. Steganography hides the very existence of a secret message and in the best nobody can see that the parties are communicating in secret. Watermarking places the information within the content where it is never removed during normal usage. In fact, watermarking techniques are particular embodiments of Steganography is not robust while watermarking has an additional feature, which is robustness (resistant to any type

of distortions) [2].

2. Proposed Method

In this work we have devised a method for data hiding (image or text) which is an improved version of already proposed algorithm by the authors which uses GÖdelization technique[1] and Modified auxiliary carry technique [4] for embedding data into the host image. In this paper we have proposed an algorithm in which we use the principle of Huffman coding [6] for encoding the secret data. The encoded string now is embedded into a cover image (original image in which data is embedded) using the modified auxiliary carry method technique. The output is a watermarked image and a binary string, which is termed as key. The sender transmits the watermarked image and the key alone is again transmitted via any public key encryption algorithm [5]. The scheme is shown in figure1 below:

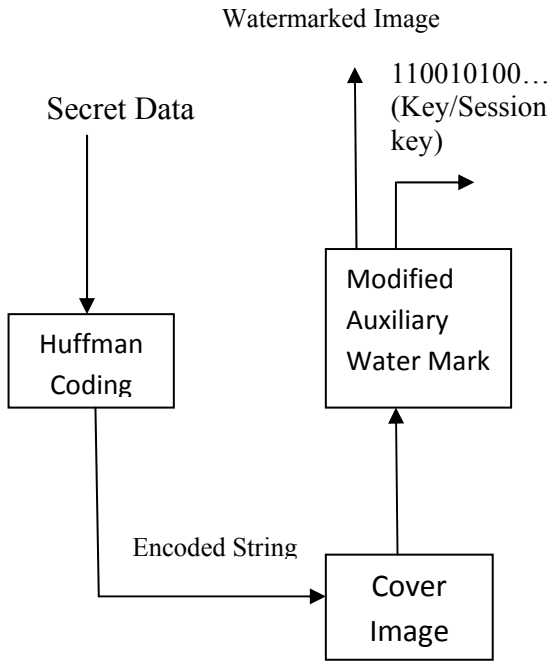


Figure1 Scheme of the proposed methodology

The above scheme can be explained as follows: The secret image or data which is the input is converted (encoded) into code words through the principle of Huffman coding. This encoded string is embedded into the original image by using the modified auxiliary carry watermarking method [4]. After this process the output will be a watermarked image and a key, which is a binary array. The key is required at the receiver end for decoding process. The key (binary array) is then transmitted using any public key encryption algorithm (like RSA encryption algorithm) [5]. The advantage of this method is that the data embedding capacity is more when compared to other well known techniques under spatial domain. The GÖdelization technique which is yet another method proposed by the authors encodes each byte of the secret data into Gödel numbers and the encoded strings are termed as GÖdel number strings. These Strings are then compressed using Alphabetic codingtechnique [1] and the output string is embedded into the host image using modified auxiliary carry techniques [4]. In this method, while encoding the secret data into GÖdel numbers, in the worst case there is a chance of the data being expanded than the actual size of the original image. So, alphabetic coding technique is used to compress the data. So keeping in view the above setback we modify the process wherein we compress the secret data using Huffman coding and then embed the data into the original image. The advantages of this method over the earlier accounts to more data hiding capacity and less complexity at the encoding side, yet providing more security through layered approach.

2.1 Overview of Huffman Coding: Huffman coding is an entropy encoding algorithm used for lossless data compression developed by David A. Huffman. The term refers to the use of a variable-length code table for encoding a source symbol (such as a character in a file) where the variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It can be informally defined as a prefix-free binary code (a set of code words) with minimum expected codeword length (equivalently, a tree with minimum weighted path length). Formally it can be defined as follows:

Input: (i) Let the input be an array of alphabet A= {a1, a2, …..an},which is the symbol alphabet of size n.

(ii) Let W= {w1,w2,……wn}, which is the set of the positive symbol weights

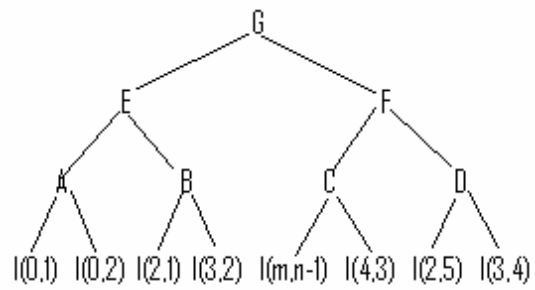
Wi=weight(ai), 1≤i≤n

Output: Code C(A,W) = {C1,C2,…..Cn}, which is the set of (binary) code words, where C_i is the codeword for a_i, 1≤i≤n. Here we use Huffman coding for encoding the secret data and then embed the encoded data into the cover image.

2.2 Data compression using Huffman coding technique: Here we consider grey level images and implement Huffman coding technique. Grey scale is a sequence of grey shades ranging from black to white with intermediate shades of grey. It ranges from (0, 2), n is the number of bits. Here we consider grey level values of 8-bit grey scale image range from 0 to 255. An image is a m*n matrix represented as:

$$I(x,y) = \begin{pmatrix} I(0,0), I(0,1)....I(0,n1) \\ I(1,0), \ I(1,1)\ldots I(1,n-1) \\ I(m-1,0),. \ldots I(m-1,n-1 \end{pmatrix}$$

Where I(i,j) denotes the intensity(I) of the pixel (i,j). Here 0≤I≤255 for an 8-bit grey scale image. In an image, a grey value may occur several number of times. Huffman coding technique is based on the frequency of occurrences of each grey value. In Huffman coding, the first is to find the frequency of occurrences of each grey value. Let the frequencies for the grey values in the image I(0,0), I(0,1), I(0,2), ... I(m,n-1) be f(0,0), f(0,1), f(0,2), ... f(m,n-1) respectively. Now place the grey values in the descending order of the frequencies. Then add the two bottommost frequencies and name the grey value of the result with an alphabet (say A). Also note the upper grey value of the two added frequencies as the left child of A and the bottom grey value as the right child of A. Now again place the grey values in the descending order of the frequencies and again add the two bottom most frequencies and name the grey value of the result as B. Also note the left and right children of B. The left and right children may be either grey value or an alphabet. Repeat the above mentioned steps until we get only two grey values at last. Now mark the grey value of higher frequency among them with the codeword as 1 and the grey value of lower frequency with the codeword as 0. Now starting with the grey values with the primary code words, construct a tree with the left and right children of the respective grey value. It must be sure that all the grey values in the image are presented in the tree representation.



The root of the tree is initially marked with the codeword '0' or '1'. Now, starting with the root, mark the left child with the codeword which is obtained by placing '0' at the right side to the codeword of the root and the right child with the codeword that is obtained by placing '1' at the right side to the codeword of the root. Follow the above method, until we get the code words for all the grey values in the image. As an example by following the above procedures, we can get some of the code words for grey values in the image as follows:

Position	Pixel Value	frequency	codeword
I(0,0)	12	100	0
I (0,1)	122	34	0110
I (0,2)	34	22	01
……..	…….	…….	…….
…	…	…	….
I (m,n-1)	65	12	00001

Thus the grey value with maximum frequency gets the codeword with minimum length and the grey value with minimum frequency gets the codeword with maximum length. Now the grey values in the image are replaced with the respective code words so as to compress the image and then the compressed secret image is embedded into the original image with the help of modified auxiliary carry method.

3. Encoding algorithm:

Step 1: Read the original image.

Step 2: Read the secret image (the intensity values of the pixels of the image) which is to be hidden.

Step 3: Starting from the first value, find the code words for each and every grey value in the image using Huffman coding technique.

Step 4: Replace the grey values in the image with the respective code words.

Step 5: Now embed the secret image with the code words into the original image using modified auxiliary carry watermark method.

Step 6: The output of step 5 is a binary string in encoded form. The code words with the grey values are also appended to the above binary string as a digital signature. This can be transmitted securely using any public key encryption technique.

4. Decoding algorithm:

Step 1: Obtain the binary array (key) and decode according to the modified auxiliary array watermark decoding algorithm. Also decode the grey values with the code words from the digital signature.

Step 2: The output of step 1 will be a sequence of characters (code words) delimited by special characters and the grey values with code words.

Step 3: The code words are replaced with the grey values.

Step 4: The image can be formed from these values.Example for this algorithm:

Step1: Read the pixel values of the original image. Let the values of the image be

120	75	220	240	200	125	75	220
241	230	130	231	215	240	233	130
230	195	200	101	100	205	100	101
211	161	171	223	230	211	151	171
65	63	125	45	36	35	95	24
3	190	161	191	150	211	240	201
200	251	171	180	211	201	230	214
150	121	230	219	210	190	222	231

Step 2: Read the secret image

0	1	0	0
2	3	1	2
3	2	1	0
1	1	2	2

Step 3: Compress the secret image using Huffman code. We consider the pixel values and their corresponding frequencies of the image as follows

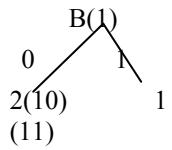
Grey values	Frequencies
2	5
1	5
0	4
3	2

Place the frequencies in descending order and add the bottom most two values and again do the descending process. Repeat the above steps until we get primary codes. A is the combined result of grey values 0 and 3. A ---> (0,3)ii) Then follow the descending order

Grey values	Frequencies
A	6
2	5
1	5

iii) B is the result of adding grey values 2 and 5
B---→ (2,5)

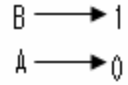
Grey Values	Grey Values
A	6
B	10



iv) Then follow the descending order

Grey Values	Grey Values
B	10
A	6

and so now the code words for A and B



are Finally the code words for grey values in secret image are

Grey Values	Code Words
0	00
1	11
2	10
3	01

Replace the code words in place of grey values in secret image .Now the secret image becomes

00	11	00	00
10	01	11	10
01	10	11	00
11	11	10	10

Step 4: Using the auxiliary method, embed the secret image into the original image. Now the original image becomes

120	73	220	241	200	125	73	220
241	230	130	231	215	241	233	130
230	195	201	100	102	207	100	100
211	161	171	225	231	210	151	170
65	63	125	45	36	35	95	24
3	190	161	191	150	211	240	201
200	251	171	180	211	201	230	214
150	121	230	219	210	190	222	231

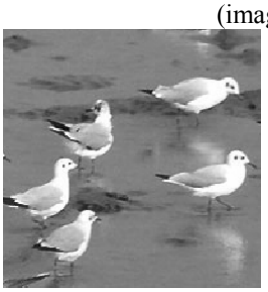
(red colored numbers indicate where the data is embedded).

Step 5: The key produced in this example is1$00$11$00$00$00$00$00$00$11$00$00$11$00$10#000#1,11#2,10#3,01.Here, the appended code words (after $ symbol) act as a Digital signature.

Experimental results:

Test case: Here the size of the cover image is 256 x 256 and the size of the Watermark is 64 x 64.

Cover image



Watermark (image to be embedded)

The resultant watermarked image is also of the same size 256 x 256

Watermarked image

5. Conclusion:

This paper proposes a watermarking algorithm which uses the technique of Huffman coding for encryption of the data and modified auxiliary carry technique for embedding the data into the cover image. Here we consider images with grey levels from 0-255.

References:

[1] D. Lalitha Bhaskari, P. S. Avadhani, A. Damodaram, "A Combinatorial Approach for Information Hiding Using Steganography And GÖdelization Techniques" , IJSCI (International Journal of Systemics, Cybernaticsand Informatics), October 2007, pgs 21-24, ISSN 0973-4864.

[2] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, "Digital Watermarking", Morgan Kaufmann publishers , 2002.

[3] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The Universityof Birmingham, "Steaganography and Digital Watermarking- A Tutorial".

[4] D. Lalitha Bhaskari, P. S. Avadhani, A. Damodaram, "Watermark Insertion Algorithm Implementation Using Auxiliary Carry And LSB methods", proc. Int.conference on Systemics, cybernatics and Informatics, Jan 3-5,2006, Hyderabad, India, pp 666-668.

[5] http ://www.mycrypto.net/ encryption/ cry pto_algorithms.html

[6] W.Bender, D.Gruhl, N.Morimoto, and A.Lu, Techniques for data hiding, IBM Systems Journal, 35(3 & 4), 1996.

About Authors:

Mrs. Dr. D. Lalitha Bhaaskari is an associate professor in the department of Computer Science and Engineering of Andhra University. Her areas of interest include Theory of computation, Data Security, Image Processing, Data communications, Pattern Recognition. Apart from her regular academic activities she holds prestigious responsibilities like Associate Member in the Institute of Engineers, Member in IEEE, Associate Member in the Pentagram Research Foundation, Hyderabad, India.

Dr. P. S. Avadhani is a professor in the department of Computer Science and Engineering of Andhra University. He has guided one Ph. D student and right now he is guiding 10 Ph. D Scholars from various institutes. He has guided more than 93M.Tech. Projects. He received many honors and he has been the member for many expert committees, member of Board of Studies for various universities, Resource person etc for various organizations. He has co-authored 4 books. He is a Life Member in CSI, AMTI, ISIAM, ISTE, YHAI and in the International Society on Education Technology. He is also a Member of IEEE, and a Member in AICTE.

M. Viswanath is a research Assistant under the guidance of Prof. P. S. Avadhani, Dr. D. Lalitha Bhaskari in the department of Computer Science and Engineering of Andhra University. His areas of interest include Data Security, Image Processing, Data Communications.