International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August 2019

High Capacity Secured Digital Watermarking for Copyright Protection

Ananthi Sheshasaayee, Sujatha D

Abstract — Computer Network provides a way to share and distribute files and information to the masses within a short span of time. With the advancement in the networking technology, many new ways to share the information is cropping up like mushrooms. With the growth in technology and ways to share information, security and authentication of the information becomes a major issue. There are many ways to secure the information shared, like Cryptography, which makes the information shared unintelligible and Steganography, which hides the data to be shared inside another digital medium like text, image, video or audio files. We propose a high capacity secured digital watermarking steganography by combining cryptography and steganography thus taking advantage of the merits of both Cryptography and Steganography. We achieve high capacity by compression and security by encryption.

Keywords — Cryptography, Compression, Information Hiding, Digital Watermarking, Encryption, Steganography

I. INTRODUCTION

Information Security is a methodology and technique practiced for securing the confidential data that is being transmitted across the insecure anonymous network. It makes the data more secure from different active and passive attacks that constantly happen during transmission. Nowadays Internet is the fast and effective way of communication in this digital era. With the growth of technology, Internet has become less costly and easily accessible that makes it more vulnerable to malicious intruders.

II. INFORMATION HIDING

Techniques or methods used to hide information can be categorized as given below:

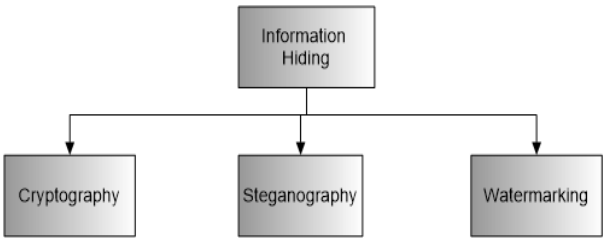

Fig. 1. Classification of Information Hiding

Revised Manuscript Received on August 30, 2019.
* Correspondence Author
Dr. (Mrs). Ananthi Sheshasaayee*, PG & Research Department of Computer Science, Quaid E Millath Govt College for Women, Chennai, India.
Sujatha D, PG & Research Department of Computer Science, Quaid E Millath Govt College for Women, Chennai, India.

Cryptography and Steganography offer a very reliable solution for such issues. Cryptography is a method that scrambles the secret data beyond understanding and thus maintains secrecy to keep the information secure. But because of this unintelligible nature of the secret, it raises suspicion and more prone to attacks. Steganography is also termed as "invisible communication" wherein the secret is kept under a media like audio, video, image and many more. In Steganography, images have been a good choice for a cover medium, because it is quite simple and secure way to transfer the information over the internet [4]. Secret message is concealed within the cover image is known as the stego image. Stego key is used for hiding the secret and also at the receiver side for extracting the hidden secret data.

Digital Watermarking is the technique of watermarking a digital file with a code, either text or another image, for the purpose of authentication and copyright protection. With the recent mammoth advancement in networking technology, it has become very easy to share files across the network and within a very short span of time, the files are being shared to millions of people living across the globe. This raises various concerns with regard to legalization and protection of data being shared. The files can be easily copied and shared with an entire different motive causing legal and communal problems, putting the rights of the owner at risk. Having a watermark in place can ensure the authenticity of the digital file and helps in copyright protection.

III. PROPOSED WORK

In the proposed system, we try to achieve high capacity secured digital image by compressing and encrypting the data to be embedded. We take advantage of the limited capability of the Human Visual System (HVS) where a slight distortion to the image is not visible to the naked eye and propose a secured method of transporting high volume of data in digital images by using cryptographic and steganographic methods. Using compression technique, we can achieve embedding more confidential data along with the copyright information which can be used later to prove the ownership of the digital file in case of any conflict. By encrypting the copyright information, we increase the security of the data transmitted over the network. We propose to employ two-level encryption on the confidential data and copyright information for better security and apply compression technique and then embed the encoded compressed data in an image to be transmitted over the open channel. The proposed system process from both the sender and the receiver side is given as block diagrams below:

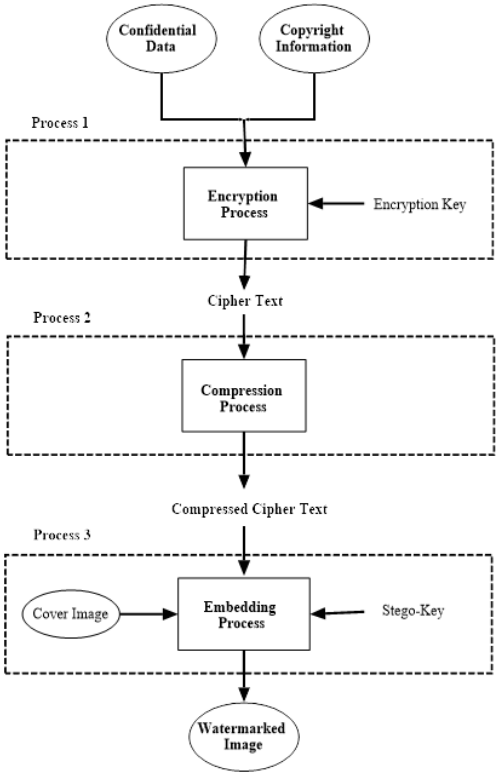

Fig. 2. Block diagram of the proposed work – Sender side

The watermarked stego image can be transmitted over the network to the receiver.

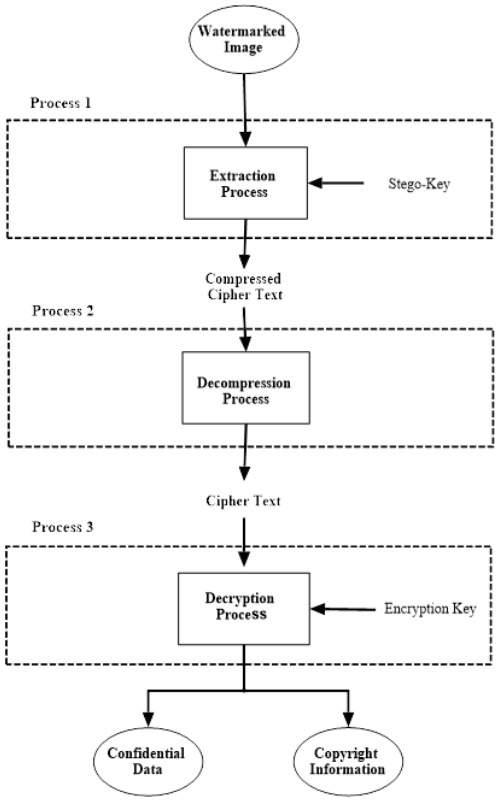

Fig. 3. Block diagram of the proposed work – Receiver side

The receiver extracts the embedded data, apply decompression and decryption techniques using the private key shared between the sender and the receiver. After verifying the authenticity of the digital file, the extracted confidential data can be used for processing by the receiver. The copyright information is used to provide the authenticity or the ownership of the file transmitted.

A. Encryption Process

There are various encryption techniques to encrypt text. The two basic techniques are symmetric and asymmetric encryption methods. In symmetric key encryption method, the same key is used for the encryption and decryption process. The algorithm chosen for encryption in the proposed system is mono-alphabetic cipher algorithm. This algorithm is a substitution cipher algorithm which for a chosen keyword the cipher alphabet for each alphabet or symbol is fixed. A table is constructed by using the letters in the keyword and other alphabets and symbols. After the keyword is filled in the table, the remaining alphabets are filled. Mono-alphabetic encoding method is chosen since it is widely used and a proven method of encryption. Due to its certain limitations, we propose to employ a two level encryption using two different keys.

The algorithm to encrypt the copyright information using symmetric key encryption technique is given below:

Table- I: Encryption Algorithm

Input: Confidential data and Copyright Information, CI; Encryption keys, K1, K2 **Output: Cipher Text, CT**
Encryption Process: Step 1: Read the confidential and copyright information, CI Step 2: Apply first level encryption on CI using K1 → CT1 Step 3: Apply second level encryption on CT1 using K2 → CT Step 4: Return cipher text, CT

B. Compression Process

There are two basic techniques to compress files, like lossless and lossy compression methods. During the compression process, certain bits could be lost resulting in lossy compression. In lossy method, we will not be able to get back the original file, whereas in lossless compression method, we can reconstruct the original file from the compressed data. Since the embedded confidential data and the copyright information will be used by the receiver for processing the data, the algorithm chosen for compression should definitely by lossless. Huffman compression algorithm is chosen based on the fact that it is lossless; it is widely used and also based on its compression ratio[3]. The algorithm to compress the cipher text using lossless compression technique is given below:

Table- II: Compression Algorithm

Input: Cipher Text, CT **Output: Compressed Cipher Text, CCT**
Compression Process: Step 1: Read the cipher text, CT Step 2: Apply compression technique using Huffman coding method on CT → CCT Step 3: Return the compressed cipher text, CCT

C. Embedding Process

Among the various domains used to embed the copyright information in a digital image, the spatial domain technique is widely used because of its high payload capacity and lesser complexity of the algorithm. The spatial domain technique modifies the pixel values of the cover image to embed the information.

In this, the Least Significant Bit method takes advantage of the 24 bits used to represent one pixel in a RGB based image file. This method embeds the secret message in the least significant bits of the pixel [1].
The algorithm to embed the copyright information in an image file using the LSB technique is given below:

Table- III: Embedding Algorithm

Input: Compressed Cipher Text, CCT; Cover Image, CI **Output: Watermarked Stego Image, SI**
Embedding Process: Step 1: Read the compressed cipher text, CCT Step 2: Read the cover image, CI Step 3: Embed CCT in CI using spatial domain technique → SI Step 4: Return the stego image watermarked with the copyright information, SI

IV. EXPERIMENTAL ANALYSIS

The proposed model is shown as a step by step process below.

A. Encryption Process using Mono-Alphabetic substitution cipher method

Keyword: "COPYRIGHT INFORMATION"

Table- IV: Cipher Text Alphabet Table

Plain Text	Cipher Text	Plain Text	Cipher Text	Plain Text	Cipher Text	Plain Text	Cipher Text
a	C		M	n	J	9	9
b	O	3	A	,	K	0	0
/	P	4	E	o	L	u	U
c	Y	i	/	p	5	v	V
d	R	j	D	7	6	!	!
1	I	/	1	8	,	w	W
2	G	k	2	q	7	x	X
e	H	l	E	r	8	?	?
F	T	5	.	:	Q	y	Z
.	N	6	3	s	:	z	
g	F	m	4	t	S		

The input to be shared/embedded in the image is given below:"This is to demonstrate the mixed monoalphabetic substitution cipher encryption which includes date and time along with the name and location. 12th July 2019 at 12:15 PM/*/sujathad/*/kingsley/*/https://goo.gl/maps/3twPqScNzGtA9xQY9"
The output after the encryption process is given below:
"sm/: /: sl rh4lj:s8csh smh 4/xhr 4ljlce5mcohs/y :uo:s/sus/lj y/5mh8 hjy8z5s/lj wm/ym /jyeurh: rcsh cjr s/4h celjf w/sm smh jc4h cjr elycs/ljn igsm duez g0i9 cs igqi. 54p1*p1:udcsmcrp1*p1 2/jf:ehzp1*p1mss5:qp1p1fllnfep14c5:p1asw57:yjfsc9x7z9"

After the decryption process, the embedded information is given below:

"this is to demonstrate the mixed monoalphabetic substitution cipher encryption which includes date and time along with the name and location. 12th july 2019 at 12:15 pm//*//sujathad//*// kingsley//*//https:////goo.gl//maps//3twpqscngta9xqy9"

Character Error Rate calculation for the encryption process:

Character Error Rate, $CER = (i+s+d)/n$ [5]

where i = no. of character insertions
s = no. of character substitutions
d = no. of character deletions
n = total no. of characters

For the above example,

Ignoring the difference in case:

CER = (10+0+0)/231 = 0.04329

Considering the difference in case:

CER = (10+11+0)/231 = 0.09091

It can be seen that the character error rate is significantly low for the given example. Lower character error rate shows better encryption/decryption technique.

B. Compression Process using the Huffmann Encoding technique

Input: Encrypted data to be embedded is stored in the file sample.txt

Output: Compressed data is stored in file sample.bin

The file size reduction is calculated using the compression ratio (CR) and space saving (SS) parameters.

$$\text{Compression Ratio} = \frac{\text{Uncompressed Size}}{\text{Compressed Size}}$$

$$\text{Space Savings} = 1 - \frac{\text{Compressed Size}}{\text{Uncompressed Size}}$$

The compression process was run for different files with increasing file size. The results are tabulated below:

Table- V: Compression ratio Table

Run No.	File size before compression	File size after compression	Compression Ratio	Space Saving
1	240 bytes	141 bytes	1.7021	41.25%
2	19,292 bytes	9,593 bytes	2.011	50.27%
3	3,85,878 bytes	1,91,860 bytes	2.0086	50.22%

It can be seen from the table above that the Huffman encoding method is efficient.

C. Embedding Process using the Spatial Domain technique

The encrypted and compressed copyright information is embedded in the cover image "Tirunelveli_canal.jpg". The cover and the stego images are given below. There seems to be no visible changes on the stego image as compared with the cover image.

Fig. 4. Cover Image

Fig 5. Stego Image

The similarity between the cover image and the stego image is measured using two techniques: Histogram and PSNR value. The histogram showing the difference in the cover and the stego-images are given below. There is only a very minor difference seen in the histogram.

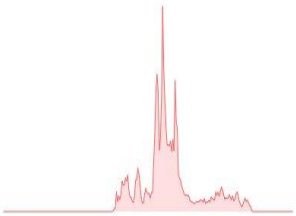

Fig. 6. Histogram of Cover Image

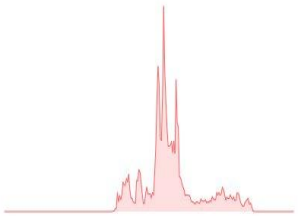

Fig 7. Histogram of Stego Image

The quality of the stego image is evaluated using the Peak-Signal-to-Noise-Ratio. Higher the PSNR value better is the quality of the image.

The PSNR value between the cover image and stego image for the various runs are tabulated below:

Table- VI: PSNR Value for the various runs

Run No.	File size of data to be embedded (bytes)	File size after compression (bytes)	PSNR Value (dB)
1	240	141	80.25
2	19,292	9,593	78.88
3	3,85,878	1,91,860	67.80

It can be seen that there is a slight decrease in the PSNR value as the volume of the data to be embedded is increased.

V. CONCLUSION

The method presented here is designed to propose a secure data hiding technique that can be used for information sharing and copyright protection. It can be used for systems requiring high volume of data to be embedded without compromising the security of the system. In this methodology, cryptographic and steganographic techniques are combined to enable a more secured information sharing mechanism between the sender and the receiver of the digital image file. By combining the capabilities of both cryptography and steganography, we achieve much greater security rather than employing just cryptography or steganography alone[10]. We try to achieve large payload capacity of the embedded information by employing spatial domain technique and also by compressing the data to be embedded. In case of any legal breach, the authenticity and the ownership of the file can be proved by extracting the copyright information from the stego image.

REFERENCES

1. Shamim Ahmed Laskar, Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012
2. Prerna Parmar, Neeru Jindal, "Image Security with Integrated Watermarking and Encryption", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p-ISSN: 2278-8735.Volume 9, Issue 3, Ver. V (May - Jun. 2014)
3. Satir, E. & Isik, H., "A Huffman Compression Based Text Steganography Method", Multimed Tools Appl (2014) https://doi.org/10.1007/s11042-012-1223-9
4. Dr. Sumathy Kingslin, R.Saranya, "Evaluative Study on Substitution and Transposition Ciphers", 2018 IJCRT, Volume 6, Issue 1 January 2018 | ISSN: 2320-2882
5. Dr. Sumathy Kingslin, R.Saranya, "Hybrid Scheme of Information Hiding Using Cryptography And Video Steganography (IHCVS)", JETIR December 2018, Volume 5, Issue 12 (ISSN-2349-5162)
6. Senthil Shanmugasundaram, Robert Lourdusamy, "A Comparative Study Of Text Compression Algorithms", International Journal of Wisdom Based Computing, Vol. 1 (3), December 2011
7. Abhishek Tiwari, Kamlesh Kumar Gupta, "An Effective Approach of Digital Image Watermarking for Copyright Protection", International Journal of Big Data Security Intelligence Vol. 2, No. 1 (2015)
8. Ahmad Shaik, V. Thanikaiselvan, Rengarajan Amitharajan, "Data Security Through Data Hiding in Images: A Review", Journal of Artificial Intelligence ISSN 1994-5450
9. Reeta Chainani, Dr. Harsh Sadawarti , G.S. Kalra, " A Review on Digital Watermarking For Copyright Protection of Digital Data", International Journal of Innovative Computer Science & Engineering, ISSN: 2393-8528
10. Khalil Challita, Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (ISSN 2220-9085)
11. Mirko Köhler, Ivica LukiT, and Višnja KriDanoviT Hik, "Protecting Information with Subcodstanography", Hindawi Security and Communication Networks, Volume 2017, Article ID 9130683, https://doi.org/10.1155/2017/9130683

AUTHORS PROFILE

Dr. (Mrs.) Ananthi Sheshasaayee, M.C.A., M.Phil., Ph.D., PGDET Is working as **Associate Professor & Head** in the Post Graduate & Research Department of Computer Science at Quaid-E-Millath College for Women, Chennai, with an academic experience of 28 years. With proven leadership skills gained from managing various large departments through problem solving, interpersonal and communication skills, and strong knowledge in current IT trends, the researcher has authored numerous books, research articles and conducted seminars, workshops and conferences. Embracing technology to help meet goals, measures performance and encouragement during discussion of expectations and standards, has helped her to produce quality researches and researchers in Computer Science. Her research methodology techniques include the knowledge of principles and practices of research ideals to effectively and ethically manage and oversee a complex problem a domain.

Ms. D. Sujatha, MCA, M.Phil, Is a Research Scholar in the Post Graduate & Research Department of Computer Science at Quaid-E-Millath College for Women, Chennai, India. She has received her Master of Computer Application Degree from Madras Christian College, Chennai, India and has her M.Phil. Degree from Periyar University, Salem, India. Her area of interest includes Information Security.