ISSN 0974 - 9373

Vol. 15(2013) Special Issue 2 **Journal of International Academy of Physical Sciences** pp. 437-443

Authentication in Stenography Using HMAC Algorithm*

Krishan Kant Lavania, Anuj Arora, Madhur Kumar Gupta and Saumitra Mani Traphati

Department of Information Technology
Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India
Email: k@lavania.in

(Received June 14, 2011)

Abstract: Steganography is the art of hiding, and transmitting information using apparently innocent carrier without expose any suspicion. This paper will take an in-depth look at this technology by comparing it with some similar techniques like cryptography and digital watermarking, and look at the least significant technique which is used to hide message in noisy bits of an image, some details on Bin Laden as Steganography Master. The paper shows work on performing authentication using HMAC algorithm on sending of message using stegnography in order to improve the integrity and authenticity of message.

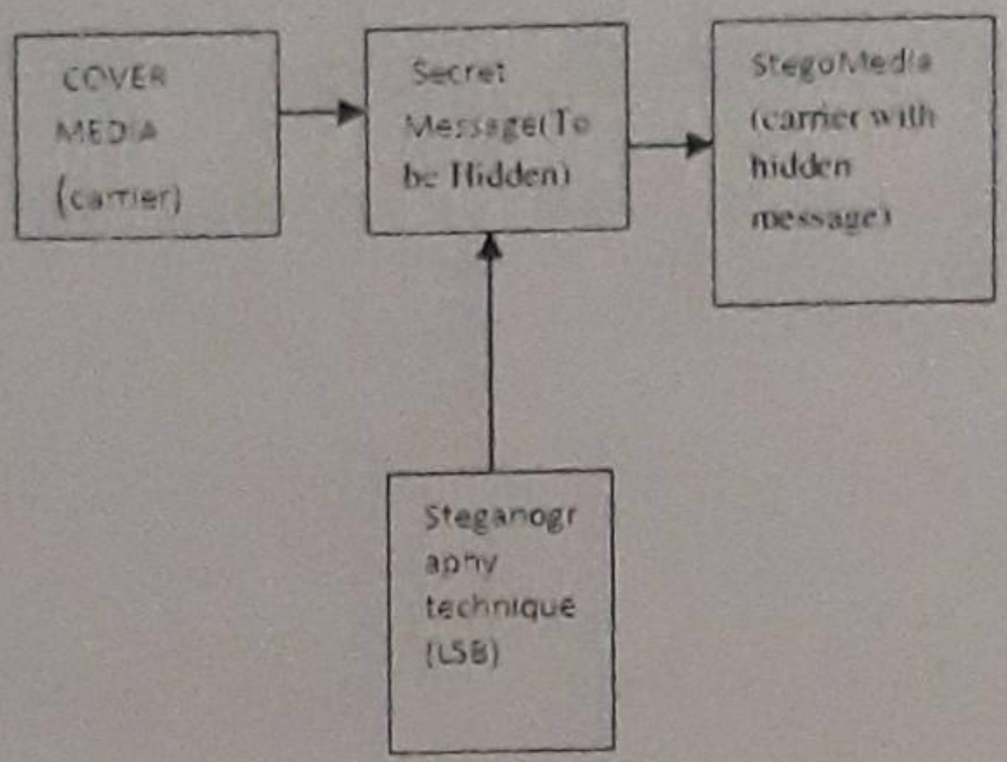
1. Introduction

Now a day steganography plays a critical role in Information Security. Steganography, from the Greek, means covered or secret writing, and is a long-practised form of hiding information. Steganography is the art and science of communicating in a way which hides the existence of the secret message communication such that the potential monitors do not even know that a message is being sent[1]. Its purpose is to hide the very presence of communication as opposed to cryptography which aims to make communication unintelligible to those who do not possess the right keys. "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." We can use digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as "covers" or carriers to hide secret messages. Information to be protected is hidden in another data known as cover or carrier. Data containing hidden message are called as Steganos or Stegos. Steganos look like cover data and it is difficult to differentiate between

*Paper presented in CONIAPS XIII at UPES, Dehradun during June 14-16, 2011

them[2-3]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Generally, the sender performs the following operations:

1. Select a non-secret cover-message.
2. Produce a stego-message by concealing a secret embedded message on the cover-message by using a stegokey.
3. Send the stego-message over the insecure channel to the receiver.
4. At the other end, on receiving the stego-message, the intended receiver extracts the secret embedded message from the stego-message by using a pre agreed stego-key.



Images stored previously in the JPEG format are a very poor choice for cover images. This is because the quantization introduced by JPEG compression can serve as a "watermark" or a unique fingerprint, and you can detect even very small modifications of the cover image by inspecting the compatibility of the stego-image with the JPEG format.

2. Comparision

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

Watermarking and Fingerprinting are the cousins of steganography. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is

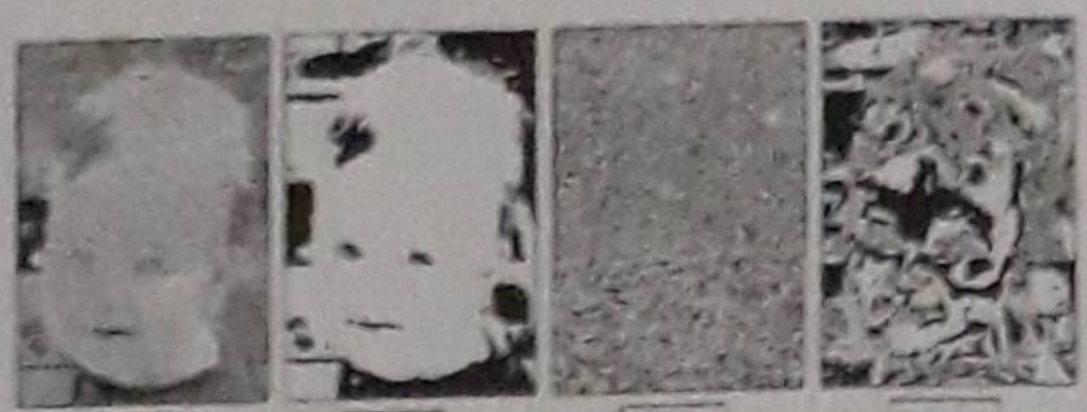
usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded indistinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties .In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge– sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial.

3. Least Significant Bit Technique

In this section we deal with data encoding in still digital images. In essence, image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image. To a computer, an image is an array of numbers that represent light intensities at various points, or pixels.

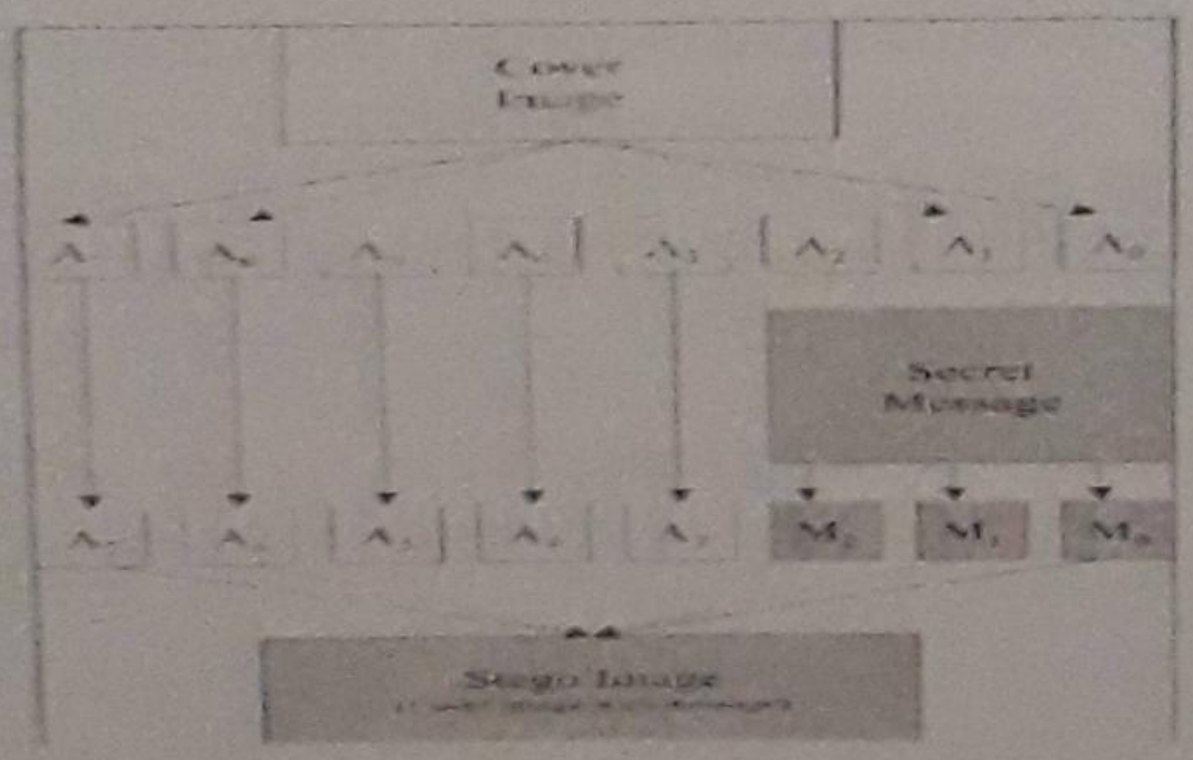
These pixels make up the image's raster data. Digital images are typically stored in either 24-bit or 8-bit per pixel fades. 24-bit images are sometimes known as true colour images. Obviously, a 24-bit image provides more space for hiding information; however, 24-bit images are generally large. As such, large files would attract attention were they to be transmitted across a network or the Internet. Image compression is desirable. However, compression brings with it other problems but, still image compression offers a solution to large image files. Two kinds of image compression are lossless and lossy compression. Both methods save storage space but have differing effects on any uncompressed hidden data in the image.

Lossy compression, offers high compression, but may not maintain the original image's integrity. This can impact negatively on any hidden data in the image. Lossy compression is frequently used on true-colour images, as it offers high compression rates. Lossless compression maintains the original image data exactly; hence it is preferred when the original information must remain intact. It is thus more favoured by steganographic technique. Each pixel is of 8 bit and carry some information. But, not all bit carry the same amount of information.



(a) 8-bit grayscale source image.
(b) Most significant bit a7 plane of the source.
(c) Least significant bit a0 plane of the source.
(d) Bit plane a4 of the source image.

Here we see only the most significant bits of an image are responsible for its vision. So we can easily embed our message in these least significant bits. By using the LSB of each byte (8 bits) in an image for a secret message, you can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. As you can see, much more information can be stored in a 24-bit image file. Depending on the color palette used for the cover image (i.e., all gray), it is possible to take 2 LSB's from one byte without the human visual system (HVS) being able to tell the difference. The only problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG)[4-5].



A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the coverobject, but the cover-object degrades more statistically, and it is more detectable. Other variations on this technique include ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color.

(hanges in these pixels are then avoided because slight changes would cause noticeable variations in the area.

Major advantage of the LSB algorithm is it is quick and easy. There has also been steganography software developed which work around LSB color alterations via palette manipulation. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity.

4. Bin Laden: Steganography Master

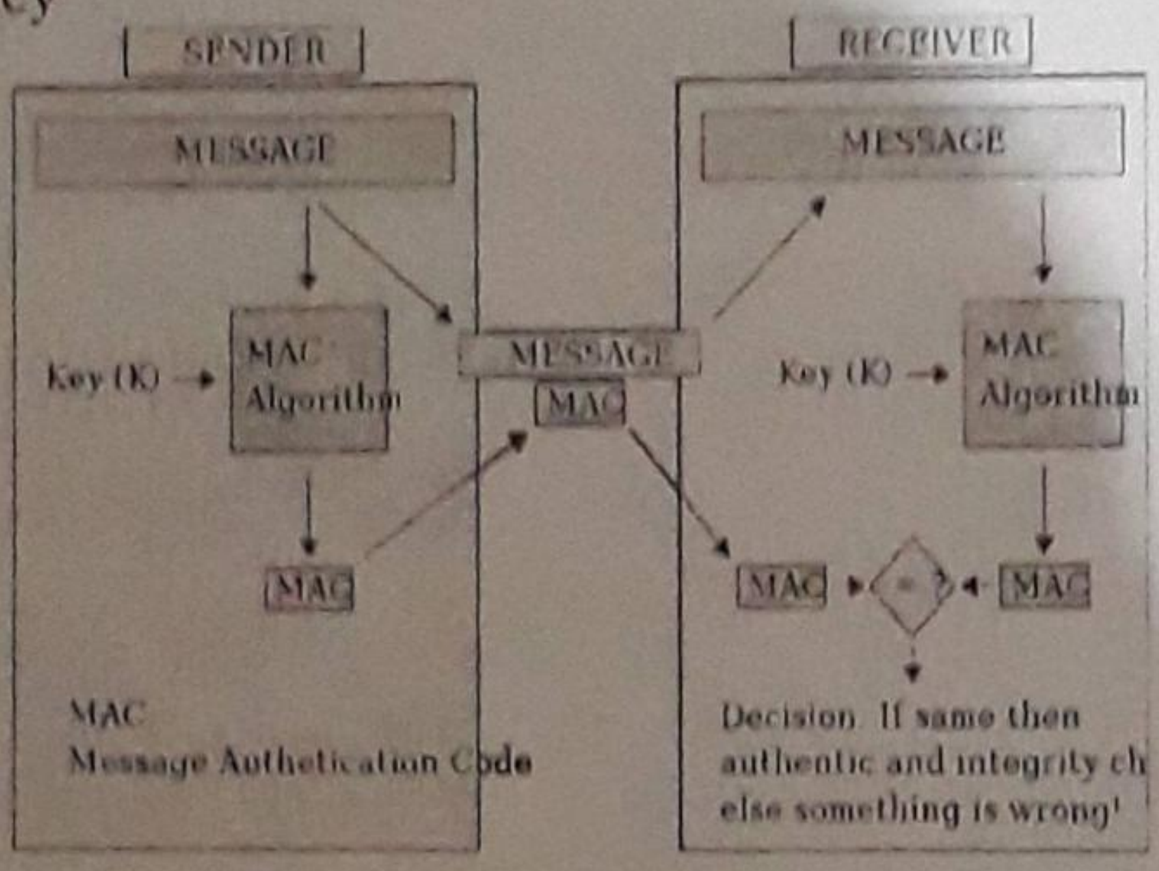
If there's one thing the FBI hates more than Osama bin Laden, it's when Osama bin Laden starts using the Internet. So it should be no surprise that the feds are getting unusually jittery about what they claim is evidence that bin Laden and his terrorist allies are using message-scrambling techniques to evade law enforcement.USA Today reported on Tuesday that bin Laden and others "are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other websites, U.S. and foreign officials say." Modern steganographers have far-more-powerful tools. Software like White Noise Storm and S-Tools allow a paranoid sender to embed messages in digitized information, typically audio, video or still image files that are sent to a recipient.

It has been noted that the Abul Nidal organization and Bin Laden's al Qa'ida organization were using computerized Internet files by methods of e-mail, steganographic, and encrypt ion to communicate to their operations. It has been reported that the alleged hijackers in the September 11th attacks had Internet email accounts and were using them to communicate with each other. Mohammed Atta, one of the alleged hijackers was repeatedly seen in a Florida library downloading pictures of children and Middle Eastern scenes which authorities suspect he used as secret method of communication.

5. Authentication in Steganography

Steganography completely based on keys. Once an intrudergets a key he can easily decrypt a message by using the key and get the original content of message. Through this confidentiality of a message break. In order to support confidentiality and improve integrity of an image we first encrypt the message which we have to transfer over the network channel. HMAC (Hash-based Message Authentication Code) is a specific construction for calculating a message authentication code (MAC) involving a hash function in combination with a secret key. As with any MAC, it may

be used to simultaneously verify both the data integrity and the authenticity of a message. Any hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The strength of the HMAC depends upon the strength of the underlying hash function, the size of its hash output length in bits and on the size and quality of the cryptographic key[6-7]



While MAC functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgeryunder chosen-plaintext attacks. This means that even if an attacker has access to an oracle which possesses the secret key and generates MACs for messages of the attacker's choosing, the attacker cannot guess the MAC for other messages without performing infeasible amounts of computation.[8]

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.

6. Conclusion

As we know earlier any sort of authentication was not posed in stegnography, which makes the sending of message unsecured. As the techniques used were much reliable but the fear of any detect of message in between was always there. So in order to keep security of message till it reaches the destination is important.

To provide authentication, we make use of HMAC algorithm which also provide data integrity along with autenticity. The output obtained is encrypted with the medium of images and send over. HMAC makes use of MD5 algorithm so detection of secret message becomes difficult. The verification of message received like in digital signature makes it much secure.

One more advantage of performing such operation is that earlier we were facing the loss of quality of medium. Now, we have improved it as the output do not affect on medium in any condition. Hence, we can say that the original message is made hide and authenticated.

References

1. www.garykessler.net/library/steganography.html
2. Stego Archive, *Steganography Information*, Software and News to enhance your Privacy, 2001.
3. Neil F. Johnson, Steganography, 2000.
4. SANS INSTITUTE, *Steganographic Techniques and their use in an Open-Systems Environment*, 2002.
5. SANS Institute InfoSec Reading Room, Steganography: Past, Present, Future.
6. http://en.wikipedia.org/wiki/HMAC.
7. csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.
8. http://en.wikipedia.org/wiki/Message_authentication_code.