ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

# A Novel Data Hiding and Image Authentication Technique for Enhanced Security

M.Renuka
M.Tech(DECS Dept),
Al HabeebInsitute of Engineering and Technology.

Shravani, M.Tech
Asst Prof,
Al HabeebInsitute of Engineering and Technology.

## ABSTRACT:

In this paper a masking based data hiding and imageauthentication technique (MDHIAT) has been proposed byembedding a message/image into a colour image. Bits fromauthenticating message/image are embedded in single bit positionunder each byte of the source image by choosing a standard 3 x 3mask in row major order. Point of insertion of a bit is obtained bycomputing modulus operation of the position of the image bytewithin the mask and an integer s whose value lies between 1 and 8.A message digest MD-5 has also been generated fromauthentication message/image and inserted into the source imagein same manner to impart additional security.Experimental results show a good fidelity in embedded imagewhen the value of s is less than equal to 6. Results are comparedwith the most popular steganographic algorithm S-Tools in termsof histogram, noise and, standard deviation analysis whereproposed MDHIAT shows better performance in compared to STools.

## INTRODUCTION:

This paper presents MDHIAT to insert messages/image inthe source image for image identification or verification. Thepresented work emphasizes on information and imageprotection against potential enemy while being transmittedacross the networks. The produced output image will be aproperly authenticated image. The fidelity of the decoded iscomparable with the source image. The scheme uses efficientinsertion of single bit within a byte in each mask of size 3 x 3,which conform proper authentication and identification of theimage. Now aday's authorised image trafficking across the network is a bigchallenge. Image authentication, identification and ownershipverification may be done though embedding message/imageinto the original image. The technique is called data hidingwithin the image. It has wide range of applications to protectthe image from potential enemy. For easy access andproliferation of network facilities it is very hard task topreserve the originality [11] of the image. There are tools andtechniques to protect the originality and to ensure theauthenticity of the image document. In this paper a noveltechnique MDHIAT has been proposed to perform the task.

## Data masking techniques:

### Substitution:

Substitution is one of the most effective methods of applying data masking and being able to preserve the authentic look and feel of the data records.It allows the masking to be performed in such a manner that another authentic looking value can be substituted for the existing value. There are several data field types where this approach provides optimal benefit in disguising the overall data sub set as to whether or not it is a masked data set. For example, if dealing with source data which contains customer records, real life surname or first name can be randomly substituted from a supplied or customised look up file.

If the first pass of the substitution allows for applying a male first name to all first names, then the second pass would need to allow for applying a female first name to all first names where gender equals "F". Using this approach we could easily maintain the gender mix within the data structure, apply anonymity to the data records but also maintain a realistic looking database which could not easily be identified as a database consisting of masked data.

This substitution method needs to be applied for many of the fields that are in DB structures across the world, such as telephone numbers, zip codes and postcodes, as well as credit card numbers and other card type numbers like Social Security numbers and Medicare numbers where these numbers actually need to conform to a checksum test of the Luhn algorithm.

## Shuffling:

The shuffling method is a very common form of data obfuscation. It is similar to the substitution method but it derives the substitution set from the same column of data that is being masked. In very simple terms, the data is randomly shuffled within the column. However if used in isolation, anyone with any knowledge of the original data can then apply a "What If" scenario to the data set and then piece back together a real identity. The shuffling method is also open be reversed if the shuffling algorithm can be deciphered.Shuffling however is a great technique to include in your overall masking approach as it has some real strengths in certain areas. If for instance, you need to maintain the end of year figures for your financial information in that test data base. You could mask the names of the suppliers and then shuffle the value of your accounts throughout your masked database. It is highly unlikely that anyone, even someone with intimate knowledge of the original data could derive a true data record back to its original values.

## Number and date variance:

The numeric variance method is very useful for applying to financial and date driven information fields. Effectively, a method utilising this manner of masking can still leave a meaningful range in a financial data set such as payroll. If the variance applied is around +/- 10% then it is still a very meaningful data set in terms of the ranges of salaries that are paid to the recipients. The same also applies to the date information. If the overall data set needs to retain demographic and actuarial data integrity then applying a random numeric variance of +/- 120 days to date fields would preserve the date distribution but still prevent traceability back to a known entity based on their known actual date or birth or a known date value of whatever record is being masked.

## Encryption:

Encryption is often the most complex approach to solving the data masking problem. The encryption algorithm often requires that a "key" be applied to view the data based on user rights. This often sounds like the best solution but in practice the key may then been given out to personnel without the proper rights to view the data and this then defeats the purpose of the masking exercise. Old databases may then be copied with the original credentials of the supplied key and the same uncontrolled problem lives on.

## Nulling out or deletion:

Sometimes a very simplistic approach to masking is adopted through applying a null value to a particular field. The null value approach is really only useful to prevent visibility of the data element.In almost all cases it lessens the degree of data integrity that is maintained in the masked data set. It is not a realistic value and will then fail any application logic validation that may have been applied in the front end software that is in the system under test. It also highlights to anyone that wishes to reverse engineer any of the identity data that data masking has been applied to some degree on the data set.

## Masking out:

Character scrambling or masking out of certain fields is also another simplistic yet very effective method of preventing sensitive information to be viewed. It is really an extension of the previous method of nulling out but there is greater emphasis on keeping the data real and not fully masked all together.This system is not very effective for test systems but is very useful for the billing scenario detailed above. It is also commonly known as a dynamic data masking method.

## Static and on-the-fly data masking:

Static Data Masking is done on the golden copy of the database. Production DBAs load the backup in a separate environment, reduce the data set to a subset that holds the data necessary for a particular round of testing (a technique called "subsetting"), apply data masking rules while data is in stasis, apply necessary code changes from source control and push data to desired environment.

## On-the-Fly Data Masking:

On-the-Fly Data Masking happens in the process of transferring data from environment to environment without data touching the disk on its way.

The same technique is applied to "Dynamic Data Masking" but one record at a time. This type of data masking is most useful for environments that do continuous deployments as well as for heavily integrated applications. Organizations that employ continuous deployment or continuous delivery practices do not have the time necessary to create a backup and load it to the golden copy of the database.

## Data Masking and the Cloud:

In latest years, organizations develop their new applications in the cloud more and more often, regardless of whether final applications will be hosted in the cloud or on- premises. The Cloud Solutions as of now allow organizations to use Infrastructure as a Service or IaaS, Platform as a Service or PaaS, and Software as a Service or SaaS. There are various modes of creating test data and moving it from on-premises databases to the cloud, or between different environments within the cloud. Data masking invariably becomes the part of these processes in SDLC as the development environments' SLAs are usually not as stringent as the production environments' SLAs regardless of whether application is hosted in the cloud or on-premises.

## Hash-based message authentication:

In cryptography, a keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic 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 cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key

## PROPOSED SYSTEM:

The proposed MDHIAT embeds authenticating message/image AIm,n of size m x n bits (maximum) for the purpose ofauthentication of the source image SIm,n of size m x n bytes.

X3 mask is chosen from the source image matrix in row majororder and single bit into each byte from authenticatingmessage/image is inserted between 1st to 6th position from LSBof the byte. The insertion positions of the authenticating bitsare calculated through a mathematical function, which dependson the absolute position of the pixel within the mask and aninteger s whose values lies between 1 and 8.At the beginningof the embedded image the size of authenticatingmessage/image is also fabricated in same fashion. As sourceimage is colour three authenticating bits are inserted in eachsource pixel using MDHIAT. Figure 1 shows the schematicdiagram of MDHIAT.

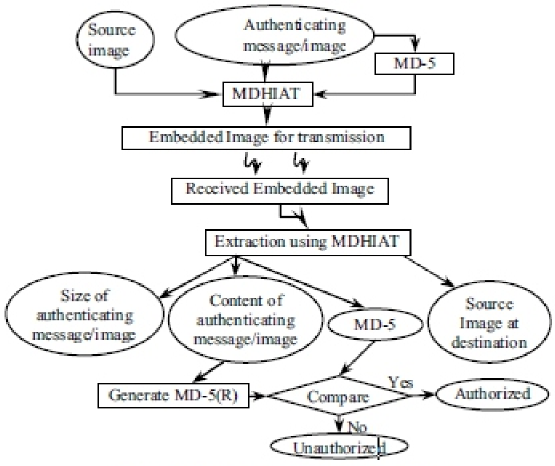
Source image
Authenticating message/image
MD-5
MDHIAT
Embedded Image for transmission
Received Embedded Image
Extraction using MDHIAT
Size of authenticating message/image
Content of authenticating message/image
MD-5
Source Image at destination
Generate MD-5(R)
Compare
Yes
Authorized
No
Unauthorized

Figure 1: Schematic diagram of MDHIAT

## Algorithm for Insertion:

The proposed scheme uses colour image as the input to beauthenticated by text message/colour image. Theauthenticating message/image bits size may be less than orequal to source image bytes.

1. Read one character/one pixel of authenticatingmessage/image at a time.

2. For each authenticating message/image byte do Read source image matrix of size 3 x 3 mask in rowmajor order.

3. Extract the message/image bit one by one.

4.Compute the position within the mask whereauthenticating message/image bit is to be inserted.

5. Replace the authenticating message/image bit in thecomputed position within the mask.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

6. Repeat step 1 and step 2 for the whole authenticatingmessage/image size, content and MD-5.

7. Stop.

## B. Algorithm for Extraction:

During decoding the embedded image has been taken as theinput and the authenticating message/image size, content andMD-5 key are extracted data from it.

1. Read embedded image mask of size 3 x 3 in row majororder.
2. For each mask do
» Compute the position within the mask in row major order where authenticating message/ image bit is available.
» Extract the message/image bit.
» Replace message/image bit position in the mask image byte by ‘1’ For each 8 (eight) bits extraction construct one character/image pixel.
3. Repeat step 1 and step 2 to complete decoding as persize of the authenticating message/image.
4. Stop.

## EXPERIMENTAL RESULTS:

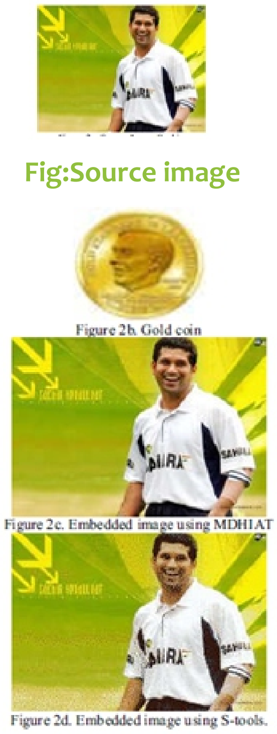

Fig:Source image

Figure 2b. Gold coin

Figure 2c. Embedded image using MDHIAT

Figure 2d. Embedded image using S-tools.

Figure 2 : Comparison of fidelity in embedding ‘Sachin’ image using MDHIAT and S-Tools

## A. Histogram Analysis:

Histogram analysis has been performed between sourceimage ‘Sachin’ and for the source image embedded with‘Gold coin’ using the MDHIAT and S-Tools.

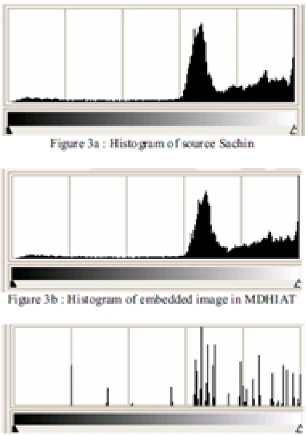

Figure 3a : Histogram of source Sachin

Figure 3b : Histogram of embedded image in MDHIAT

Figure 3c Histogram of embedded image in S-Tools

Figure 3 : Histogram for source image ‘Sachin’ embedded with ‘Gold coin’ using MDHIAT and S-Tools

## B. Noise Analysis:

Noise analysis has also been perfored for the embedded‘Sachin’ image using MDHIAT and S-Tools algorithms. Figure4 shows the pictorial representation of computation of noise.Noise is computed by finding the average of 4 direct neighbor pixels in the 3 x 3 pixels (figure 5) around the pixel Pi as givenin equation (1), where PiE and PiS are the pixel values of thepixel i in both the embedded image and source imagerespectively, and (m x n) is a number of pixels in the source.

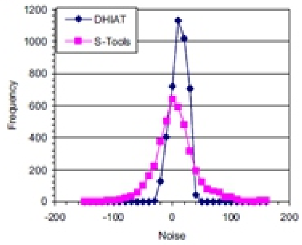

Figure 4 : Noise analysis of the image ‘Sachin’ after embedding using MDHIAT and S-Tools

## CONCLUSIONS:

In this paper the proposed image authentication techniqueMDHIAT is performs the authentication process usingmathematical operations on 3 x 3 masks to insert bits into thesource image byte. The insertion is done through maskselections in row major order for the entire image matrix; itprovides the extra level of security.

From the analysis of theresults it is clear that the image quality (like brightness,sharpness) distortion is negligible up to the modulus 6. As allare embedded within the source image like size ofauthenticating message/ image, content of it and MD-5 keywithin the source image no other information is needed fordecoding at receiver end. Different types of comparison likehistogram analysis, noise analysis, and standard deviationanalysis are performed to compare the MDHIAT with S-Toolsalgorithm. Through analysis of various results obtained fromthe implementations it reveals that the proposed MDHIAT mayresults better authentication in steganographic field.

## REFERENCES:

[1] Nameer N. EL-Emam, "Hiding a large Amount of data with HighSecurity Using Steganography Algorithm," Journal of ComputerScience ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.

[2] P. Amin, N. Lue and K. Subbalakshmi, "Statistically secure digitalimage data hiding," IEEE Multimedia Signal Processing MMSP05,pp. 1-4, Shanghai, China, Oct. 2005.

[3] B. Chen and G. W. Wornnel, "Quantization index modulation: Aclass of provably good methods for digital watermarking andinformation embedding," IEEE Trans. On Info.Theory, vol. 47, no.4, pp. 1423-1443, May 2001.

[4] R. Chandramouli and N. Memon, "Analysis of LSB based imagesteganography techniques," Proc. of ICIP, Thissaloniki, pp. 1019-1022, Greece, 2001.

[5] C.Y. Lin and S. F. Chang, "A robust image authentication methodsurviving JPEG lossy compression," Proc. SPIE, vol. 3312, SanJose, pp. 296-307, Jan. 1998.

[6] S. Dumitrescu, W. Xiaolin and Z. Wang, "Detection of LSBsteganography via sample pair analysis," In: LNCS, vol. 2578,Springer-Verlag, New York, pp. 355-372, 2003.

[7] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis ofinformation Hiding," IEEE Trans.On Info. Theory, vol. 49, no. 3,pp. 563-593, March 2003.

[8] S. Pavan, S. Gangadharpalli and V. Sridhar, "Multivariate entropydetector based hybrid image registration algorithm," IEEE Int.Conf. on Acoustics, Speech and Signal Processing, Philadelphia,Pennsylvania, USA, pp. 18-23, March 2005.

[9] H. H. Pang, K. L. Tan and X. Zhou, "Steganographic schemes forfile system and B-tree," IEEE Trans. On Knowledge and DataEngineering, vol. 16, pp. 701-713, Singapore, June 2004.

[10] P. Moulin and M. K. Mihcak, "A framework for evaluating thedata-hiding capacity of image sources," IEEE Transactions onImage Processing, vol. 11, pp. 1029-1042, Urbana, Illinois, Sept.2002.

[11] C. Rechberger, V. Rijman and N. Sklavos, "The NIST-cryptographic Workshop on Hash Functions," IEEE Security &Privacy, vol. 4, pp. 54-56, Austria, Jan-Feb 2006.

[12]S-Toolshttp://digitalforensics.Champlain.Edu/download/stools4.zip. Access Date:16.08.07.P2PiP4P3 P1