International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp 7217-7222

An Attack on Image Authentication: Unaltered Histogram

Muni Sekhar V[I], R.Sarika[II], Ch. Sravan Kumar[III], K V Rao[IV], N Sambasiva Rao[V]
Vardhaman College of Engineering, shashabad[I,II,III,] GNITS, Shaikpet[IV], SRIT Women[V] Hyderabad, Telangana State, India.

Abstract
In this paper we are defining an unaltered histogram attack to identify the problem on image authentication hash function for image content authentication. The histogram based hash function reported in literature [18, 20, 21, 22] are robust against Content Preserving Manipulations (CPM) as well as incidental distortion such as a lossy compression and a noisy transmission. The major drawback of literature techniques is that, they are not sensitive to small Block-wise Content Manipulation (BCM) without affecting histogram. Here, we proposed an unaltered histogram attack that cannot be identified by image authentication hash function that is proposed by Choi YS [3] and Vadlamudi LN [22].
The main objective of our paper is to prove the problem in histogram based authentication techniques [3, 22] among the many challenges in an image authentication. To prove the problem, we are performing BCM without modifying histogram of that image. Here, BCM is defined as block wise transpose operation. In this technique we can find the change using Human Visual System (HVS) in stego image, but not in the histogram and as well as an image hash. Here, HVS model is used by multimedia processing experts to deal psychological and biological process to measure image perceptual quality.

Keywords: Unaltered Histogram attack, Hash Function, Image Authentication, Watermark

INTRODUCTION
Now-a-day's digital communication has particularly grown and practice of digital data such as images, audios and videos. Its usage has been improved in these days, so it has become confront to provide security to the digital data. There are numerous techniques which provide security to these digital data, but there are few problems that have been acknowledged and the solution in order to solve the problem is briefly specified in [1, 2, 3, 4, 5].

MOTIVATION
The image fidelity is particularly important in sensitive applications like health care and finance, where it is significant and often a necessity for receiver, to make sure that the image is authentic without any malicious tampering. Some of the applications of image authentication also include court evidence, insurance claims, journalistic photo graphs, and so on. For instance, in applications of the courtroom evidence, when an image is provided as evidence, it is desirable that this image has not been tampered. In electronic commerce, when we purchase multimedia data from the Internet, we need to know whether it comes from the alleged producer and must be assured that no one has tampered with the content.
That is to say, the fidelity of an image is required for the image to be digital evidence or a certified product. This requirement made us work in image authentications and it is possible attacks.

PRELIMINARIES
Following are the Preliminaries of an image authentication technique:

- **Image:** An image is a rectangular grid of pixels. It has a definite height and a definite width counted in pixels. Each pixel is a square and has a fixed size on display.
- **Histogram:** It is a graphical representation of frequency distribution of numerical data (pixels).
- **Authentication:** It is a verification of the legality of a document or signature, to make it valid.
- **Hash Function (HF):** A function it maps data of any size into data of fixed size.

Organization of the paper as follows, section 2, briefly elaborates the literature and existing system. In section 3, detail discussion on problem statement. In section 4, implementation and result analysis of unaltered histogram attack and section 5, conclusion and future work.

LITERATURE SURVEY
With inconceivable growth in digital communication systems, providing integrity to the digital data is a challenging task. Here, digital data includes text, images, audio, video, etc.., will be distributed through the insecure medium (Internet) that gives vulnerability to the data. In insecure medium, there is a chance for an attacker to modify or tamper the data during transmission. To provide integrity to data and for secure transmission, various methods exist. They are broadly categorized into two types 1) Watermark and 2) Hash Function based methods. The first category watermark methods [4, 8, 14] embed secure information into a digital data. Later, the embedded information is extracted to verify the integrity of data. The second category hash function based methods [12, 17] generate a digital hash from the data using existing conventional crypto hash algorithms. The obtained hash is used to check data integrity and prevent malicious attacks.

EXISTING SYSTEM
The existing system does uses the above procedures, but the problem with crypto hash methods is that, they are very sensitive to change of data, i.e.., even there is a change in one bit of input data, drastic changes occur in the output of the crypto hash algorithm. Digital data is very large in size and requires additional computational cost to generate a hash from

the data [3, 18, 20, 21, 22]. Moreover, it is also a time-consuming process. An alternative way for providing integrity to digital data is Content-Based Authentication (CBA) [5] and Content-Based Image Authentication (CBIA) [6] are approaches that extract image characteristics or content of human perception and uses them in authentication to identify images as fabricated or a copy of the original version. The extracted characteristics like edges, textures, content information, etc.., are processed with a secret key for generating a secure hash [7]. The hash is transmitted to the receiver either by appending or embedding it to an original image or by a secure communication channel. The receiver uses the same hash generation procedure to generate hash from the received image [15, 16]. The two hashes (receiver generated and sender generated) are compared (using verification process) to check the integrity and authenticity of images. The principal goal of CBIA method is to extract robust features, which are sensitive to Content Changing Manipulations (CCM) and insensitive to incidental distortion as well as allowable Content Preserving Manipulations (CPM) [19]. The generated hash from robust features must fulfill the performance requirements of a hash method including Robustness, Fragility, Key dependent and Unbreakable [9, 10, 11, 13].

PROBLEM STATEMENT

The main objective of this work is to define a novel attack on hash function for an image content authentication using unaltered histogram attack. In this, we are taking LN Vadlamudi [22] presented a hash function to launch unaltered histogram attack.

In which [22] "*divide an image into non-overlap blocks and dispenses histogram bins of the image block into containers based on the unfinished Sum of pixel count of histogram bins. It generates Intermediate Image Hash (IIH) and followed by Binary Hash (BH), then they are compared and generate the final image hash".*

Lets us take an example of 96x96 image '*A*' as shown in figure 1 (a). Perform a transpose operation on '*A(33:64, 65:96)*', then it becomes as shown in figure 1 (b). Here, if we generate hash for 32x32 block or greater block-sizes, hash value will be same, but image content will be different. This problem we are defining is an *unaltered histogram attack*.

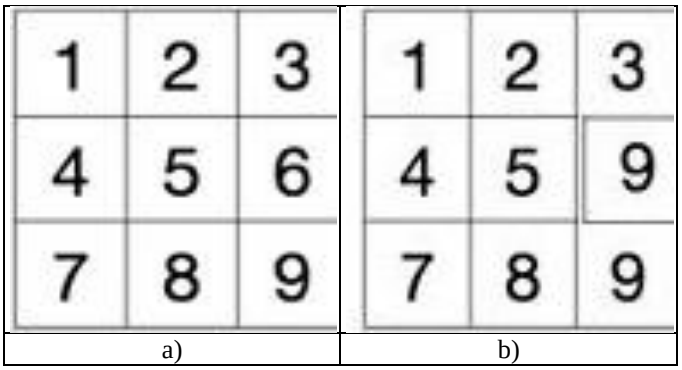


Figure 1: a) Original Image Histogram b) Modified Image and Histogram

The existing system uses the hash function that is generated by using histogram. The problem with histogram has two different images with same histograms can have the same has hash value.

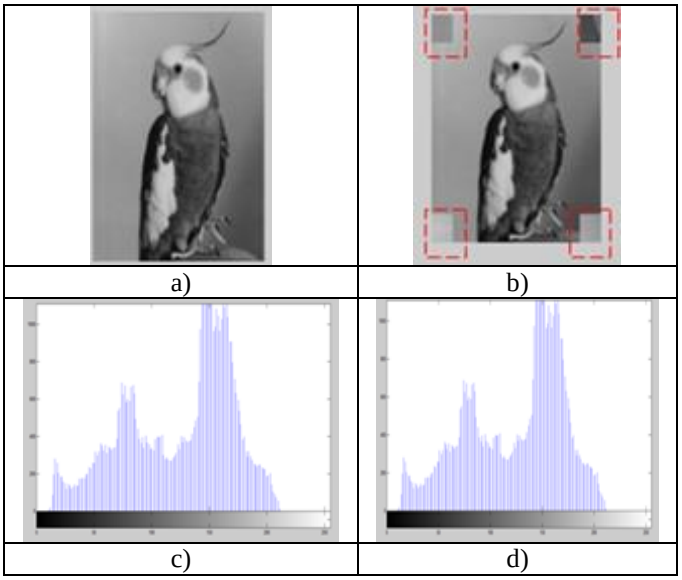


Figure 2: a) Original image b) Modified image c) Histogram of original image and d) Histogram of modified image

In above figure 2 (a) original image, after transforming of top-left, top-right, bottom-left and bottom-right corners of 32x32 block we will obtain modified image figure 2 (b). It is observed that both modified and original images have the same histograms and even after four 32x32 block-wise transform of original images.

LN Vadlamudi [22], Choi YS [3] and et al.., are proposed authentication hash functions that are based on block-wise histograms bins. In any two blocks, if the pixel values are the same then the histograms are also same. In an unaltered histogram attack we only transform pixels positions not the pixels values, so it is guaranteed that unaltered histogram attack can't be identified with small block-wise transforms.

IMPLEMENTATION AND RESULT ANALYSIS

The general design of any authentication hash functions as shown in figure 3. Here, input image I is preprocessed (convert the input image into algorithm accepted form), then generate block-wise histogram bins (IIH) followed by image hash.

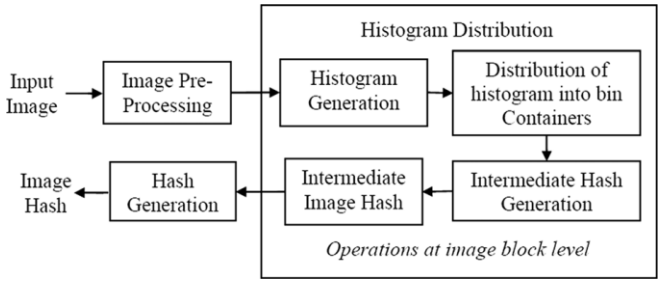


Figure 3: Block diagram image hash generation

VERIFICATION OF HISTOGRAM HASH

The general verification of histogram is done as shown in figure 4. In verifier part, if any disputes arise on image content authentication, then take that image, generate image hash to that image and compare with previous generated image hash. Whereas previous generated image hash and verifier generated image hash should use same algorithm. Previous generated image hash may use quantum key distribution algorithm for image hash to send to the verifier in secure manner [23]. Otherwise, image hash value can be hiding within the image content in none-zero DWT plus adaptive quantization intervals [24, 25].

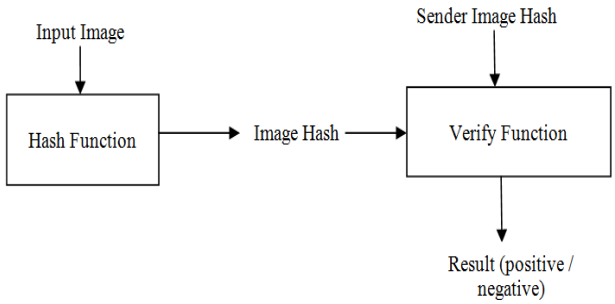


Figure 4: Verification process

STEP BY STEP ACTIVITY FLOW OF ATTACK

The basic activity flow of an unaltered histogram attack as shown in fig. 5, it has following basic steps; First identify the portion of content in targeted image, second, transform the pixels according to the need in the identified portion without changing pixel values, third generate image hash and fourth verify image hash of modified image and original image. If original image and modified image hashes are equal then unaltered histogram attack is successful, otherwise unsuccessful.

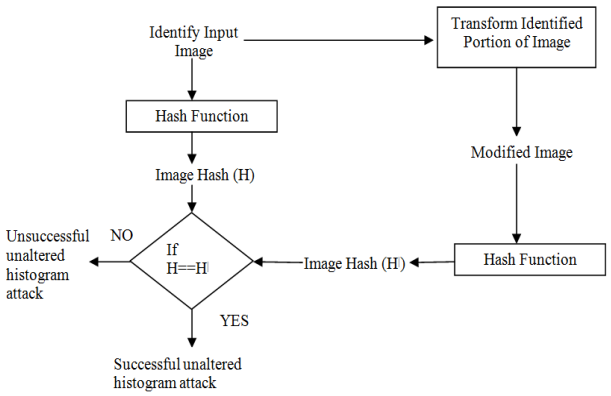


Figure 5: Flow chart of unaltered histogram attack

ALGORITHM OF UNALTERED HISTOGRAM ATTACK

Input: Original_image I , stego_image S
Output: Hash for both images is same

Algorithm Histogram_Equalization_Attack(I)

{

1. *Read* I
2. *Generate Histogram to* I *images*
3. *Calculate Modified image i.e.., by applying transpose to any of L x L matrix in input image* $L \in (4,8,16,...,128)$
4. *Generate Histogram to* S
5. *Then, the hash for original and modified image is generated.*
   hash1=Hash (Original_image);
   hash2=Hash (Modified_image);
6. */*Then the hash generated using the hash function is compared using Exclusive-OR operation */*
   if (hash1!=hash2)
   Print ('Image is modified');
   else
   Print ('Image is not modified');
   Endif

}

EXAMPLE

Let us consider an 4x4 image block (A) and its transpose (A^T) as shown in table 1 & 2 and apply the algorithm, then show the histogram of image block A and transposed image block (A^T).

Table 1: An 4 x 4 image block

A=	161	160	161	160
	161	161	161	161
	159	160	159	160
	159	160	159	160

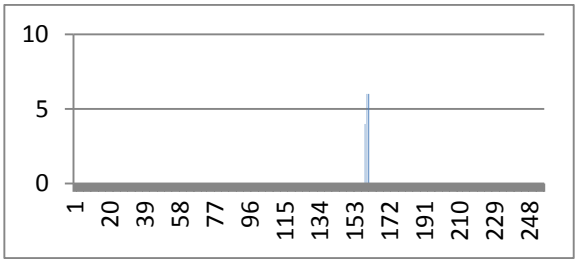


Figure 6: Histogram of the variable 'A'

And here B=A^T for the below pixel values histogram is as follows:

Table 2: An 4 x 4 transformed image block

B=	161	161	159	159
	160	161	160	160
	161	161	159	159
	160	161	160	160

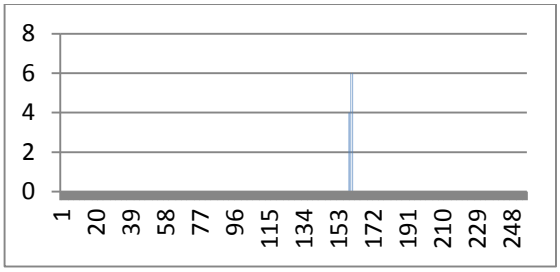


Figure 7: Histogram of the variable 'B'

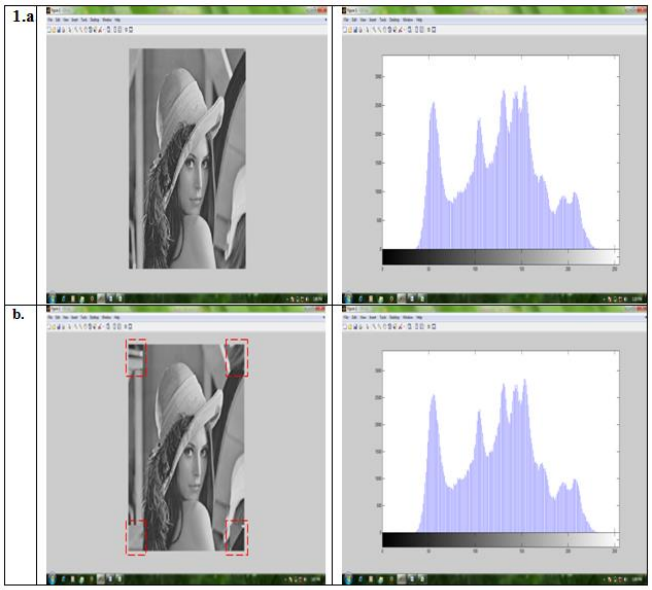
From the figure 6 & 7, it is clear that transform operation not generating any modification in block of histogram. If the same transformation operation is applied for different block sizes, then there might be possibility of same hash value in original image and modified image. It violates the image authentication property of content integrity.

RESULTS

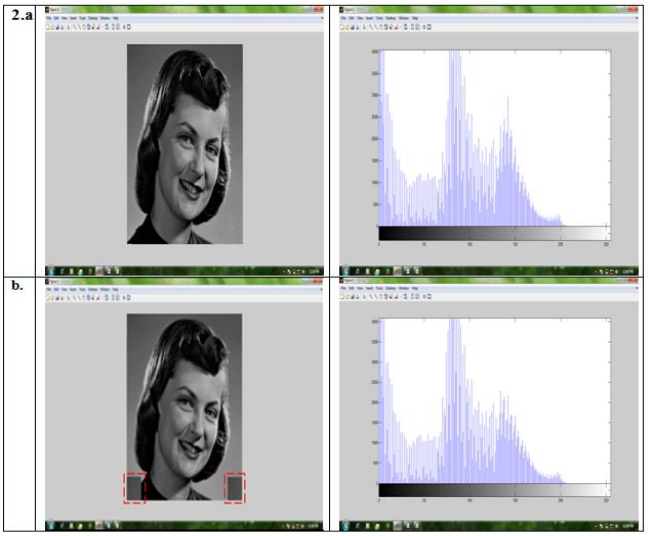
This attack is experimented with the following methods [3, 21, 22] and with two evaluation parameters such as

1) block-size and
2) True Positive Rate (TPR).

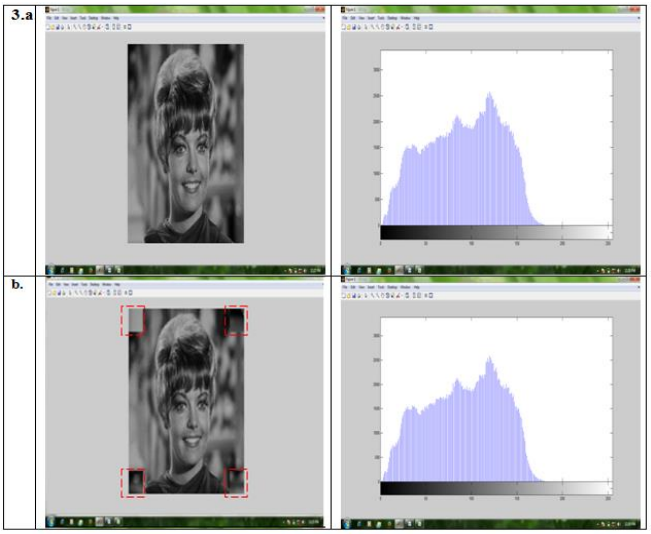
Table 3 gives percentage of TPR with in specified block-size and methods. Figure 8 show the results obtained by applying unaltered histogram attack.



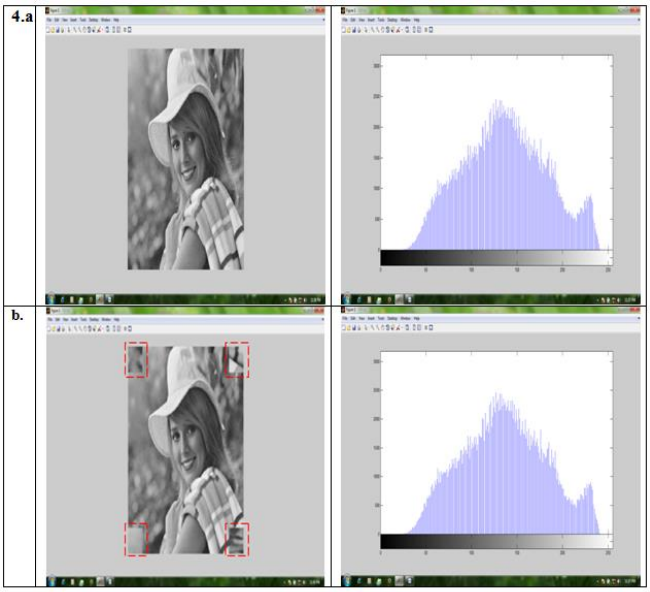
1. a. Original image and its histogram b. Modified image and its histogram



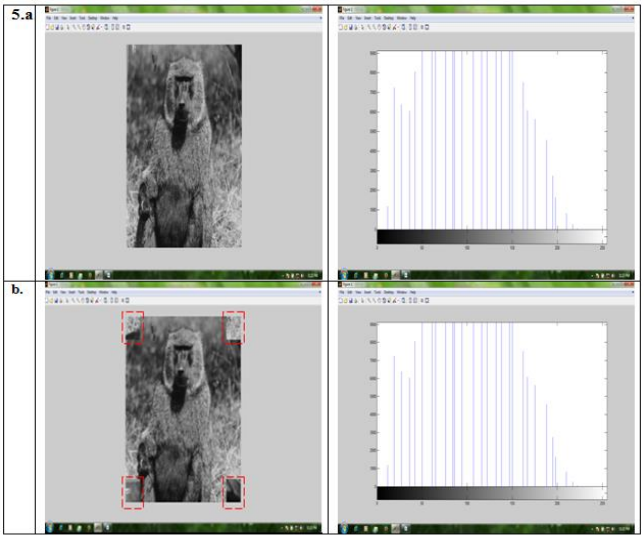
2. a. Original image and its histogram b. Modified image and its histogram



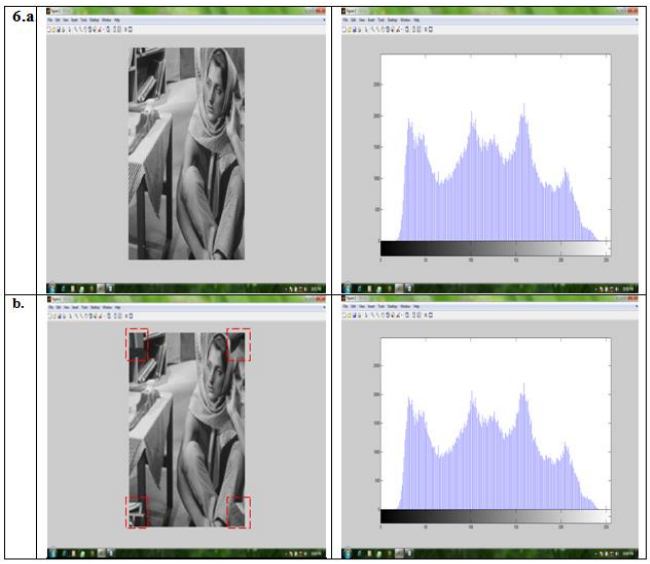
3. a. Original image and its histogram b. Modified image and its histogram



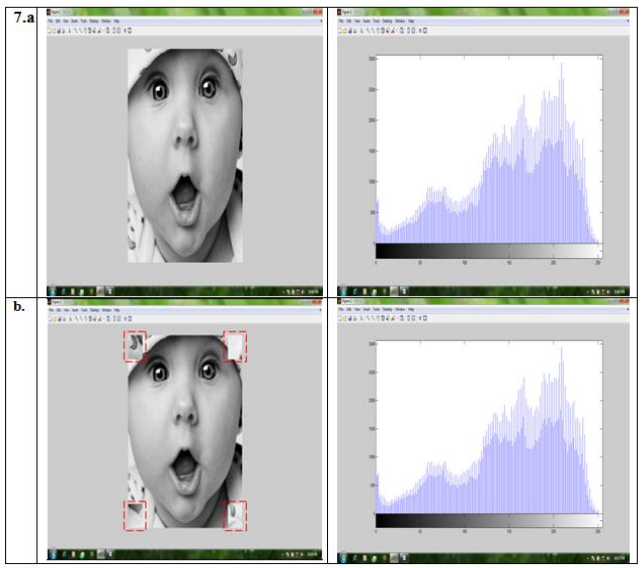
4. a. Original image and its histogram b. Modified image and its histogram



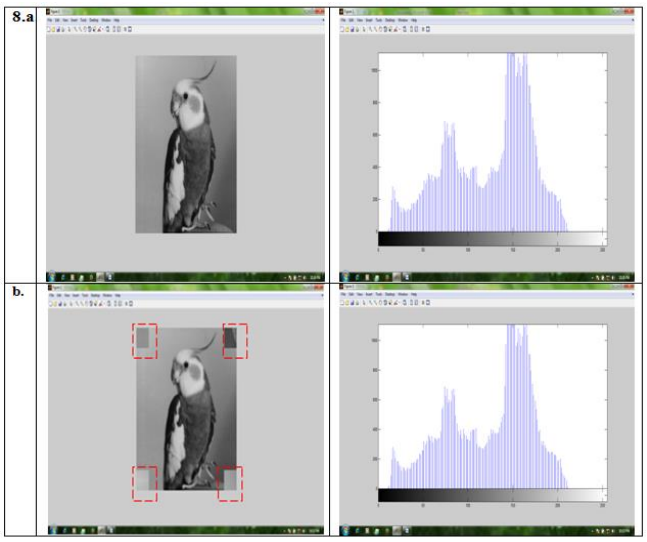
5. a. Original image and its histogram b. Modified image and its histogram



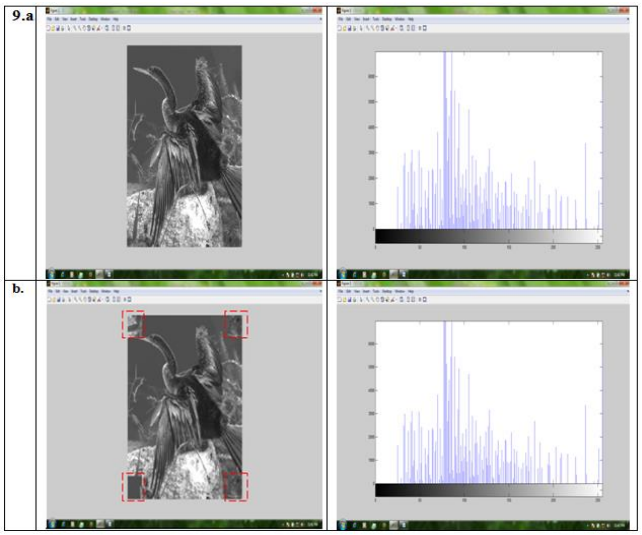
6. a. Original image and its histogram b. Modified image and its histogram



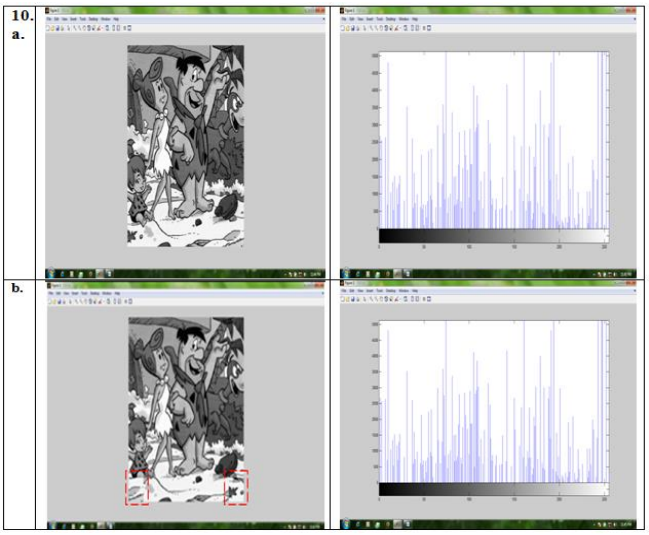
7. a. Original image and its histogram b. Modified image and its histogram



8. a. Original image and its histogram b. Modified image and its histogram



9. a. Original image and its histogram b. Modified image and its histogram



10. a. Original image and its histogram b. Modified image and its histogram

Figure 8: Result analysis

Table 3: Image authentication TPR

Method	Block-sizes						
	4	8	32	64	128	256	512
LN Vadlamudi [22]	0	0	0	0	100	100	100
Choi YS [3]	0	0	0	100	100	100	100
Xiang S [21]	0	0	100	100	100	100	100

CONCLUSION

In this paper we introduced an unaltered histogram attack on image authentication. Previously many techniques had proposed, but there are vulnerable at some point. According to this paper, the problem is specified in terms of 'Block Based Unaltered Histogram' i.e., even after image has modified within block, the histogram for the original and the modified images are same for the specified block-size. It clearly states that if we change pixel positions without changing the pixel values, then some of the image authentication techniques will not recognizes.

With the invention of unaltered histogram attack present image authentication techniques are vulnerable to small block transforms.

FUTURE WORK

To prevent block based content modification a robust image authentication technique is need to be developed. It generates authentication hash with the position information and content preserving information.

REFERENCES

[1]. Ammar M. Hassan, et al.., 2009, "Semi fragile image authentication using robust image hashing with localization," in proc. of second int. Conf Mach pp-133-137.

[2]. Black, PE., 2005, "Fisher-Yates shuffle, dictionary of algorithms and data structures," Nat. Inst Stand Technology, retrieved 2007.

[3]. Choi, YS., Park, JH., 2012, "Image hash generation method using hierarchical histogram," Int. Multimedia Tools Appl 61(1):181-194.

[4]. Goljan, M., et al.., 2001, "Distortion-free data embedding for images," in proc. of the 4th Int. Workshop Inf Hiding 25-27, pp 27-41

[5]. Han, S-H., Chu, C-H., 2010, "Content-based image authentication: current status, issues and challenges," Int. Inf Secur 9(1):19-32

[6]. Han-Ling Zhang, et al.., 2009, "Content based image hashing robust to geometric transformation," in proc. Of second Int. Symp Electron Commer Secur 105-108

[7]. Haouzia, A., Noumeir R, 2008, "Methods for image authentication: a survey," J Multimedia Tools Appl 39(1): 1-4

[8]. Leest, A., et al.., 2003, "Reversible image watermarking," in proceedings of the ICIP03. 2:731-734

[9]. Lei, Y.,et al.., 2011, "Robust image hash in radon transform domain for authentication," J Signal Process Image Commun 26(6):280-288

[10]. Wang, L., et al.., 2011, "Image authentication based on perceptual hash using Gabor filters," J Soft Comput 15(3): 493-504

[11]. Liu, G., et al.., 2011, "A passive image authentication scheme for detecting region duplication forgery with rotation," J Netw Comput Appl 34(5):1557-1565

[12]. Matsuo, T., Kaou, K., 2004, "On parallel hash functions based on block ciphers," Proc IEICE Trans Fundam Electron Commun Comput Sci E87A(1):76-74

[13]. Nighat, J., Arshad, A., 2010, "A unified approach to secure and robust hashing scheme for image and video authentication," in proc. of 3rd Int. Congr Image and Sig Process 274-278

[14]. Qi, X., Qi, J., 2007, "A robust content based digital image watermarking scheme," J Signal Process 87:1264-1280

[15]. Saad SM., 2009, "Design of a robust and secure digital signature scheme for image authentication over wireless channels," IET Inf Security 3(1):1-8

[16]. Xiang, S., et al., 2007, "Histogram based image hashing scheme robust against geometric deformations," in proc. of 9 Int. Work Multimedia and Secur 121-128

[17]. Skala, V., Kucha, M., 2001, "The hash function and the principle of duality," Proc Int Conf Comput Graph Int 200:167-174

[18]. Sun, R., ZengW,2012, "Secure and robust image hashing via compressive sensing," in Int. J Multimedia Tools Appl 1-1

[19]. Swaminathan, A., Mao, Y., Min, W., 2006, "Robust and secure image hashing," IEEE Trans Inf Forensics Secur 2(1):215-230

[20]. Weng, L., Preneel, B., 2011, "A secure perceptual hash algorithm for image content authentication," Commun Multimedia Secur LNCS 7025:108-121 Multimed Tools Appl

[21]. Xiang, S., Kim, HJ., 2011, "Histogram based image hashing for searching content-preserving copies," Trans Data Hiding Multimedia Secur VI LNCS 6730:83-108

[22]. LN., vadlamudi, et al.., 2015, "Robust hash generation technique for content-based image authentication using histogram," Published in Int. journal of Multimedia Tools Appl Vol.74(1).

[23]. Muni Sekhar, V., et al.., 2015, "Passive Attack Resistive Key Distribution Scenario: QKD," In: IJAER Vol. 10(1) pp 927-936.

[24]. Muni Sekhar, V., et al.., 2015, "Enhanced Adaptive Data hiding in DWT," In IOSR Journal of Computer Engineering Vol 17(2) pp 30-40 DOI: 10.9790/0661-17263040.

[25]. Muni Sekhar, V., et al.., 2015, "Comparing the Capacity, NCC and Fidelity of Various quantization Intervals on DWT," International Conference on Innovations in Computer science & Engineering(ICICSE-2015), published in Journal of Advances in Intelligence Systems and Computing, Springer ISBN 978-981-10-0417-9, August 2015.