

An Improved Authentication Scheme for Passport Verification Using Watermarking Technique

V. Madhu Viswanatham¹, Galma Santosh Reddy², Potluri Jagadeesh³, Mothe Dinesh Reddy⁴

¹ School of Computing Science and Engineering, VIT University
Vellore, TamilNadu-632015, India

² School of Computing Science and Engineering, VIT University
Vellore, TamilNadu-632015, India

³ School of Computing Science and Engineering, VIT University
Vellore, TamilNadu-632015, India

⁴ School of Computing Science and Engineering, VIT University
Vellore, TamilNadu-632015, India

Abstract

The prominent problem in passport authentication is to authenticate the passport document for its owner. The critical factor of this authentication procedure is to establish a correspondence between Passport's photo and its owner. A passport document contains holder details in supplement to the holder's signature. We propose an authentication scheme by extracting some details of the holder including passport number, converting them into a watermark and digesting them in a form by applying some techniques that can be hidden in the passport's photo. The computers have revolutionized the passport authentication process by using the computer in fixing the passport photo on the passport document during the issuing of passport and also verifying the passport at checkpoint by scanning. During the issue of passport, a watermark can be created based on the details of the holder full name and passport number and it can be hidden in the passport photo using watermarking technique. With the help of this technique, during the passport verification process at the checkpoint, computer can be used in scanning the passport photo to check whether the passport photo has been replaced by comparing the invisible watermark hidden in the passport photo with the holder's details including the full name and passport number.

Keywords: *Steganography, Robustness, Authentication, Watermarking*

1. Introduction

1.1. Steganography

It is a technique [5] of hiding messages so that no one can detect message existence except sender and receiver. It is a technique of providing security through obscurity. The purpose of steganography technique is to keep the existence of the information secret. The main goal of steganography is to communicate securely in a completely undetectable manner. Information can be embedded in a text file, an image, audio file or video file. Information can be embedded in an image by making minute changes to the image so as to make the information imperceptible. Manipulating or destroying the digital media [7] with the intent of destroying the hidden message is an easier task when compared to detection of presence of hidden information. Any digital media can be destroyed whether hidden information exists or not. The most successful hiding method is one which is obscure and is not vulnerable to simple attacks [8]. Due to rapid advancement in technology, computer security has to reinvent itself to meet the challenges of changing technologies, evolution of new viruses and discovery of new threats. So there is a great need for evolution in steganography, which is one of the disciplines of computer security to invent robust algorithms to withstand the new attacks.

2. The problem

2.1. Digital watermarking

Digital watermarking [2] [3] is a technique for embedding information into a digital signal (might be a audio, image or video signal) in order to provide identity of owner. Watermarking technique should satisfy the following requirements [1].

A. Robustness

The embedded information is said to be robust [2] [3] [6] if its presence can be reliably detected even after the image has been modified, but not destroyed beyond recognition.

B. Invisibility

The difference between digital media with hidden information and without information should be made invisible [2][6] to the human eye.

C. Undetectability

The embedding information is undetectable if an attacker is unable to read the hidden message given the detailed description of the source and presence of hidden information.

D. Security [4]

Attacker should be incapable of removing information embedded in the signal even though he/she knew the algorithm.

The recent procedure in issuing a passport document is by using the computer in fixing the passport photo. All the passport offices are connected through a network to exchange information to verify the correctness and authenticity of the passport. Passport images can also be transferred between offices to verify the authenticity of the passport holder.

The main problem is how to confirm the authenticity of the passport photo with the holder's details. The passport document contains holder's signature in addition to the holder's details. But there is no association between the passport photo and the passport owner details. So a passport photo can be replaced with other person's photo. Hence the purpose of the improved authentication scheme is to establish a firm connection between the passport photo and passport details.

3. Existing algorithm

The aim of the existing algorithm [1] is to provide a firm association between the passport holder's photo and the holder's details. The existing algorithm used the watermarking technique to create an association between the passport photo and holder's details by embedding hidden information in the passport photograph.

The existing algorithm [1] [7] uses the holder's first name, second name, third name, family name and passport number and converts into an invisible watermark. This invisible watermark is embedded inside the passport photo such that it satisfies all the requirements of the

watermarking technique. This process is carried out during the issue of the passport document at the passport office.

The existing algorithm consists of three algorithms. The first algorithm [1] [5] deals with acquiring the required parameters for creating the watermarking. The second algorithm [1] converts the holder's details into a watermark that can be embedded into the digital image. The third algorithm [1] hides the watermark obtained inside the passport photo such that it meets the requirements of the watermarking.

3.1. Drawbacks

1. Due to rapid advancement in technology, new tools were invented to compare original image and Steganography image to detect the presence of hidden information in a Steganography image. Suppose a Steganography image is created by applying the above algorithm, values of row, Rcolumn can be obtained by comparing original image [4] with Steganography image. Suppose key is 3 digit number, first name is 3 letters (say 'Ram'), by applying the above algorithm an attacker shall be able to obtain an equation

$$18*\text{codeval}(1)+1*\text{codeval}(2)+13*\text{codeval}(3)=\text{row}$$

It is an equation in 3 variables and can easily be solved for the values codeval(1),codeval(2),codeval(3)

Having the full knowledge of the algorithm, an attacker can be able to crack the key value by running a program on super computers by trial and error method.

So, the above algorithm does not satisfy the security requirement of watermarking.

2. In step 2 of algorithm 3, large value of pixel (row, column) is calculated. Suppose RGB value of the pixel is (0,0,0) max will be assigned value '0'.In step 3 of algorithm 3,sum is divided by max, which result in an exception division by zero.

4. Modification of Existing algorithm

4.1. Algorithm 1: Acquire Parameters

1. Get holder's first name, second name, third name and surname.
2. Get holder's Passport Number.
3. Validate the holder's details.
4. Assign a number to each letter of the name according to the table 1.
5. Store each name's numbers for future reference

Table 1. Alphabets and their equivalent code values

Character	Codeval	Character	Codeval	Character	Codeval	Character	Codeval	Character	Codeval
A	1	G	7	M	13	S	19	Y	25
B	2	H	8	N	14	T	20	Z	26
C	3	I	9	O	15	U	21		
D	4	J	10	P	16	V	22		
E	5	K	11	Q	17	W	23		
F	6	L	12	R	18	X	24		

4.2. Algorithm 2: Watermark

1. Consider the key value. E.g. $K = "1,2,3,4"$.
2. Create a new key value for first name by summing the consecutive key values in a round robin fashion say $K1$.
 Where $K1(1)=K(1)+K(2)$
 $K1(2)=K(2)+K(3)$
 $K1(3)=K(3)+K(4)$
 $K1(4)=K(4)+K(1)$

Compute the summation of the first name by adding the code value of each character multiplied by the new key's character in succession.

E.g. $codeval(1)*K1(1) + codeval(2)*K1(2) + codeval(3)*K1(3)+.....$

3. Consider the result as "row".
4. Create a new key value for second name by summing the alternate key values in round robin fashion say $K2$.
 Where $K2(1)=K(1)+K(3)$
 $K2(2)=K(2)+K(4)$
 $K2(3)=K(3)+K(1)$
 $K2(4)=K(4)+K(2)$

Compute the summation of the second name by adding the code value of each character multiplied by the new key's character in succession.

E.g. $codeval(1)*K2(1) + codeval(2)*K2(2) + codeval(3)*K2(3)+.....$

5. Consider the result as "column".
6. Compute the summation of the third name and family name by adding the code value of each character multiplied by the actual key's character in succession. E.g.
 $codeval(1)*K(1) + codeval(2)*K(2) + codeval(3)*K(3)+.....$
7. Compute the summation of passport number by adding the code value of each character. E.g. $codeval(1) + codeval(2)+ codeval(3)+.....$
8. Compute the sum of third name, family name and the passport number and store the result in "sum".

4.3. Algorithm 3: Hide Watermark

1. Get the pixel value at (row, column) location from the original Image.
2. Find the average value of RGB [6] color for that pixel, add 1 to it and assign it to "avg".
3. Divide "sum" on "avg" to get number of pixels.
4. Compute the modulo division of "sum" over "avg" and store result in "value".
5. Calculate Rcolumn which is equal to "column" + "number of pixel" + 1.
6. Get the pixel value at location (row, Rcolumn).
7. Get the largest value of (R,G,B) for the pixel at that location and replace it with "value".
8. Restore the pixel (R,G,B) values at the same location.

4.4. Algorithm 4: Authenticate

1. Select the image for which watermarking is to be applied.
2. Read the passport number for which the authentication is to be performed.
3. Perform row, column and sum computations as shown in algorithm 2 by retrieving the details from the database based on the passport number.
4. Compare the row, column and sum values obtained with the values stored in the database
5. If the step 4 is successful, perform number of pixels and value computations as shown in algorithm 3 and compare the results with the values stored in the database.
6. If the step 5 is successful, allow the holder to travel otherwise take legal proceedings on the passport holder.

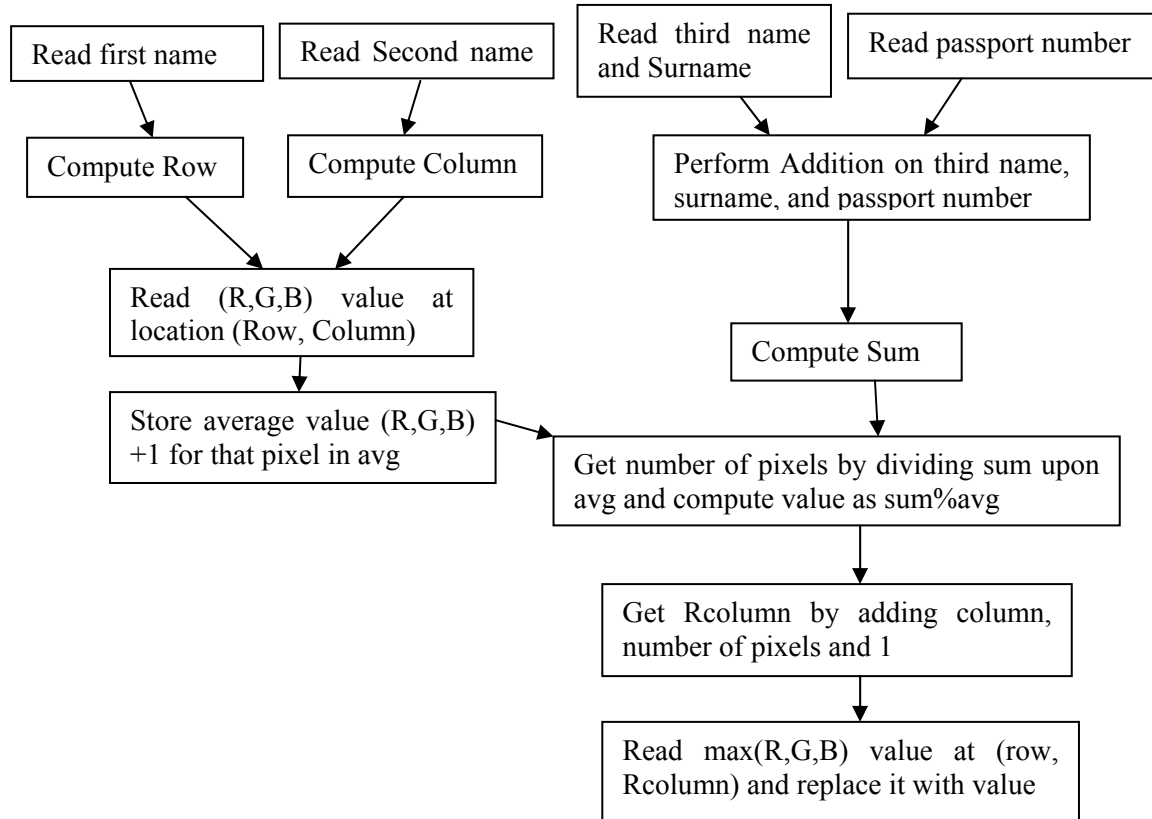


Figure 1. Flow chart for the improved algorithm

5. Analysis

The passport authentication system architecture overview is as shown in the Figure 2.

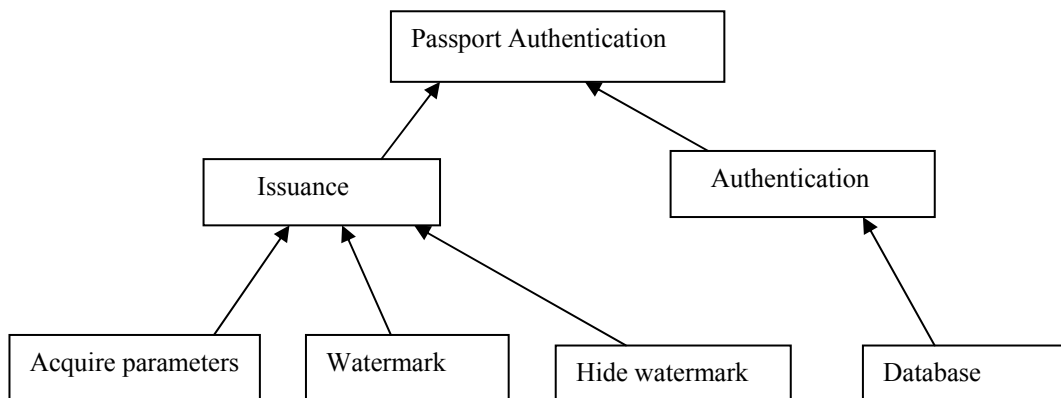


Figure 2. Passport Authentication system architecture

The passport authentication system dataflow diagram is as shown in the Figure 3.

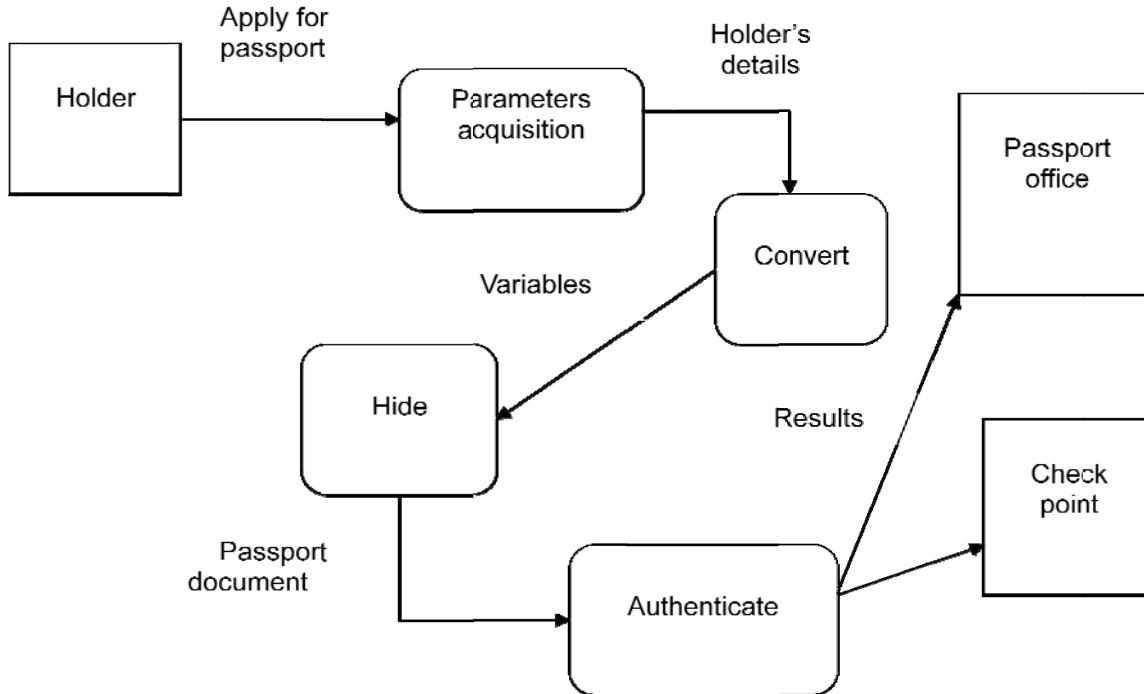


Figure 3. Passport Authentication System data flow diagram

Algorithm one will accept the passport holder full Name and his passport number for the creation of watermark, which is validated to make sure that all the information given is correct.

Each letter in the full name is assigned a codeval chosen from table 1. This table contains the alphabets and their equivalent numbers. The following equation can be used to compute the code value for each character:

$$\text{Codeval (character)} = \text{ASCII value(character)} - 64.$$

By the end of algorithm one each name (first, second, third and surname) has a sequence of numbers assigned to the each name depending on the length of name.

Algorithm two starts by selecting a key K (e.g. 1, 2, 3, 4) and then calculating the Key value for each name according to the algorithm as follows

For first name, a separate key value is calculated (say K1) as

$$K1(1) = K(0) + K(1)$$

$$K1(2) = K(1) + K(2)$$

$$K1(3) = K(2) + K(3)$$

.....

For second name, a separate key value is calculated (say K2) as

$$K2(1) = K(0) + K(2)$$

$$K2(2) = K(1) + K(3)$$

.....

For third name and surname, actual key value is taken into consideration.

Then the value for each name is calculated by multiplying code value for each character by corresponding key digits arranged in sequence and summing up the values. For the passport number each digit is converted to a code value and is summed in a sequence.

E.g. $\text{codeval}(1) * K1(1) + \text{codeval}(2) * K1(2) + \dots$ for the first name and
 $\text{codeval}(1) * K2(1) + \text{codeval}(2) * K2(2) + \dots$ for second name and
 $\text{codeval}(1) * K(1) + \text{codeval}(2) * K(2) + \dots$ for third name, surname .

$\text{pno}(1) + \text{pno}(2) + \text{pno}(3) + \dots$ for passport number

where pno refers to the passport number.

The following equation could be used to calculate value for each name

$$J = m$$

$$I = n$$

$$\sum_{I=1}^n \text{codeval}(i) * K(j)$$

$$I = 1$$

$$J = 1$$

Where, n=length of name and m= length of key.

And K refers to K1 for first name, K2 for second name and K for third name and surname.

Suppose first name is JAGADEESH

Second name is KUMAR

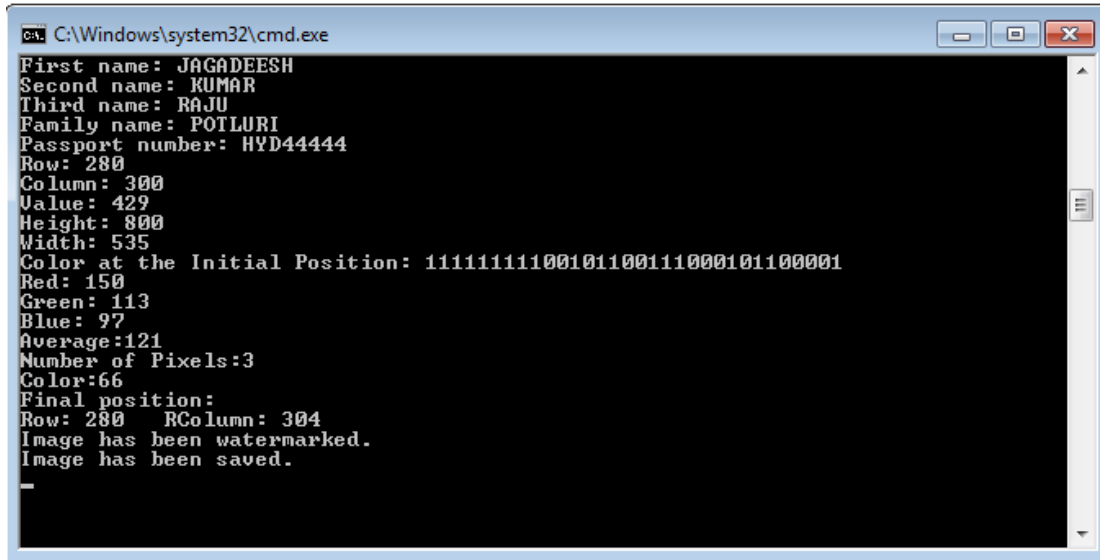
Third name is RAJU

Surname is POTLURI

Passport number is HYD44444
Actual Key value is 1234
Value of JAGADEESH is row=280
Value of KUMAR is column=300
Value of RAJU is 134
Value of POTLURI is 238
Value of passport number is 57
Value of sum = 429

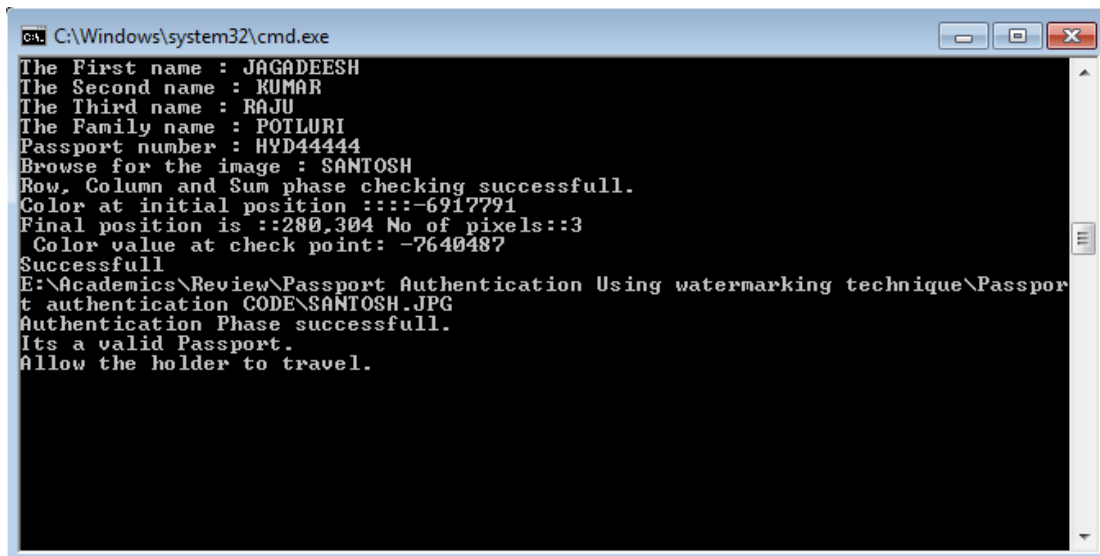
The algorithm three is for the hiding the watermark obtained during algorithm two. According to this

algorithm we read the value of the pixel at location (row, column) from the actual passport photo. Then we find the average value of (R,G,B) color for the pixel, add 1 to it and we call it "avg". After we divide the "sum" on "avg" to obtain the number of pixels. We use modulo of "sum" over "avg" to get "value". Then we calculate the new column for the pixel to be hidden i.e. Rcolumn as column + number of pixels + 1. Then value of max(R,G,B) for pixel(row,Rcolumn) is replaced with value.



```
C:\Windows\system32\cmd.exe
First name: JAGADEESH
Second name: KUMAR
Third name: RAJU
Family name: POTLURI
Passport number: HYD44444
Row: 280
Column: 300
Value: 429
Height: 800
Width: 535
Color at the Initial Position: 1111111100101100111000101100001
Red: 150
Green: 113
Blue: 97
Average:121
Number of Pixels:3
Color:66
Final position:
Row: 280 RColumn: 304
Image has been watermarked.
Image has been saved.
```

Fig.4 Implementation of passport generation module



```
C:\Windows\system32\cmd.exe
The First name : JAGADEESH
The Second name : KUMAR
The Third name : RAJU
The Family name : POTLURI
Passport number : HYD44444
Browse for the image : SANTOSH
Row, Column and Sum phase checking successfull.
Color at initial position :::-6917791
Final position is ::280,304 No of pixels::3
Color value at check point: -7640487
Successfull
E:\Academics\Review\Passport Authentication Using watermarking technique\Passpor
t authentication CODE\SANTOSH.JPG
Authentication Phase successfull.
Its a valid Passport.
Allow the holder to travel.
```

Fig.5 Implementation of passport authentication module

Improved algorithm has an advantage over existing algorithm in terms of security. The improved algorithm uses different keys for first name, second name and third name, family name which does not allow intruder to crack

key given the full knowledge of algorithm. So it satisfies the security requirement of watermarking. Also improved algorithm overcomes the divide by zero exception that may occur in the existing algorithm by adding positive

quantity(1) to the avg. So the improved algorithm overcomes the drawbacks of the existing algorithm.

6. Conclusion

This discussion has suggested an improved authentication scheme for passport authentication using watermarking technique. This authentication scheme embeds the invisible watermark into the passport photo to authenticate the passport's owner. This modified scheme meets all the requirements for the watermark technique. The invisible watermark has satisfied the robustness [2][3], Invisibility, Undetectability [2][3], and Security requirements. Because this technique has used only one pixel for hiding the watermark, it satisfied the robustness against image compression. The detection of presence of hidden information is a daunting task as it is time consuming to predict the key value. So it satisfies the security requirement of watermarking. It also satisfies invisibility requirement because change in one pixel is not visible to the human eye. The watermark also satisfies the Undetectability [3] requirement since the pixel size is very small compared to the size of an image and is not easily noticeable. This method is effective and meets all the requirements of watermarking. This scheme is applicable for only one State. So to make the authentication scheme globally feasible, every state should share keys using asymmetric key cryptography. Every state should use the public key to hide the watermark during the issue of passport and private key should be used during the verification process at the checkpoint to check the authenticity of the passport.

7. References

- [1] AlaaH.Al-Hamami and SaadA.Al-Ani, Faculty of Information Technology, Amman Al-Ahliyya University, Amman, Jordan "A New Approach for Authentication Technique"Journal of Computer Science 1 (1): 103-106, 2005 ISSN 1549-3636 © Science Publications, 2005
- [2] ManjitThapa, Dr.Sandeep Kumar Sood, A.P Meenakshi Sharma "Digital Image Watermarking Technique Based on Different Attacks". (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 4, 2011
- [3] Er. Deepak Aggarwal, Er. Kanwalvir Singh Dhindsa "Effect of Embedding Watermark on Compression of the DigitalImages" JOURNAL OF COMPUTING, VOLUME 2, ISSUE 2, FEBRUARY 2010, ISSN 2151-9617
- [4] Christian S. Collberg, Member, IEEE Computer Society, and Clark Thomborson, Senior Member, IEEE "Watermarking, Tamper-Proofing, and Obfuscation Tools for Software Protection" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 28, NO. 8, AUGUST 2002
- [5] Stefan, K. and F.A.P. Petitcolas (Eds.), 2000. Information Hiding techniques for steganography and digital watermarking. ISBN 1-58053-035-4 © Artech House, Inc.
- [6] Rafael C. Gonzalez and Richard E. Woods, 2001 "Digital image processing", second edition ISBN 0-201-18075-8Prentice hall publications
- [7] ZoranDuric, Michael Jacobs, SushilJajodia*Center for Secure Information SystemsGeorge Mason UniversityFairfax, VA 22030*"Information Hiding: Steganography andSteganalysis"
- [8] T. Pevny' and J. Fridrich STEGANOGRAPHY AND DIGITAL WATERMARKING Determining the stego algorithm for JPEG images

Dr.V.Madhu Viswanatham Currently working as Associate Professor, School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu. Obtained Ph.D from S.K. University. Areas of interest include Cryptography, Network Security and information Retrieval system. Published Research papers in the area of Network Security, MANET and Image Processing.

Galma Santosh Reddy Currently pursuing B.Tech Computer Science and Engineering in VIT University. Member of Computer Society of India VIT student branch. Research interests include Image Processing and Information Security.

Potluri Jagadeesh Currently pursuing B.Tech Computer Science and Engineering in VIT University.

Mothe Dinesh Reddy Currently pursuing B.Tech Computer Science and Engineering in VIT University.