International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-6, August 2020

(3, 3) Visual Cryptography for Online Certificate Authentication

Tridib Chakraborty, Sudeep Ghosh, Trishita Ghosh, Chowdhury Md. Mizan, Suparna Karmakar

***Abstract:** Today organizations face a challenge while recruiting candidates, who provide forged mark sheets in order to get a job. To prevent wrong hiring a detailed and thorough approach is needed to verify the authentication of both the candidate and the marks obtained by him/her. There are so many modern cryptographic protocols available which can be used for authenticating individual's academic achievement certificates. Visual Cryptography is a simple and secure way to allow the secret sharing of images without any cryptographic computations or the use of encryption or decryption keys. The novelty of the visual secret sharing scheme is in its decryption process where human visual system (HVS) is employed for decryption of secret shares. In this paper we have discussed (3, 3) visual cryptography scheme which can be used to generate shares and distributes them among three parties, i.e. the Job Seeker, Certificate Issuance Authority and the Organization conducting Job interview. Secret message can be decrypted only if all the three shares are available. Every certificate carries a unique number which is encrypted using visual cryptography and without handshaking of all the parties it is impossible to decrypt, thus ensuring full proof authentication.*

***Keywords:** (k, n) Visual Cryptography, Digital Authentication.*

I. INTRODUCTION

Presently producing fabricated Marksheet to recruiting bodies by jobseeker has transformed into a noteworthy issue. A mark sheet is said to be forged when a candidate, not holding that degree or engravings claims to hold the same. It is done by copying the certification no. of some other candidate, holding a comparable capacity truly or by changing imprints.

Making a forged imprint sheet is not a major issue these days. There are different programming projects accessible to satisfy the prerequisites of making a fabricated mark sheet.

The methodology of this paper is to distinguish fabricated mark sheet utilizing Visual Cryptography.

Visual Cryptography is a method for screening a picture which coordinates to certain shares and are doled out to specific people. At the point when these shares are incorporated the first picture is revealed.

Revised Manuscript Received on July 15, 2020.
* Correspondence Author

Mr. Tridib Chakraborty*, Assistant Professor, Department of Information Technology , Guru Nanak Institute of Technology, Nagpur, Maharashtra, India. E-mail: tridib.chakraborty@gnit.ac.in

Mr Sudeep Ghosh, Assistant Professor, Department of Information Technology, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India. E-mail: sudeep.ghosh@gnit.ac.in

Mrs. Trishita Ghosh, Assistant Professor, Department of IT, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India. E-mail: trishita.ghosh@gnit.ac.in

Miss.Suparna Karmakar, Assistant Professor, Department of IT, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India. E-mail: Suparna.karmakar@gnit.ac.in

Chowdhury Md Mizan Assistant Professor, Department of IT, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India. E-mail: chowdhurymd.mizan@gnit.ac.in

Consequently, this VC method is founded on the Human Visual System, which gives a superior method to verify pictures with no computational trouble. This recreation is finished utilizing the XOR activity. For distinguishing forged mark sheet we will incorporate
3 shares of a Certificate no.(kept verified uniquely at Certificate Issuing Body's end) and will appoint these shares to (Share 1)Certificate issuing Organization,(Share 2)Printed on Marksheet,(Share 3)candidates as an Authentication Key. The candidate or the job seeker is producing the original certificate just if in the wake of consolidating all these 3 shares the unscrambled picture matches with the first Certificate No.

From the start, the certificate issuing organization creates the Marksheet with mark sheet no imprinted on it. For each Marksheet no Issuing organization will keep a one of a kind Certificate no(associated with that marksheet no.), which will never be unveiled to competitor or jobseeker, selecting bodies or another person. One more thing, in addition, each certificate no. will hold the marks, the understudy got, as a suffix. Utilizing Visual Cryptography(VC) 3 shares will be created from this certificate no.,one of which(Share 1)will consistently be kept at Issuing Organization's hand,another one(Share 2) will be imprinted on the Marksheet and the last one (Share3) will be given to the up-and-comer or occupation searcher as Authentication Key.

Presently during the confirmation procedure of the jobseeker, the person in question will produce the mark sheet no and the authentication key to the recruiting body. They will bring the online entrance, made for recognizing forged mark sheet. Entrance will at that point bring the certificate issuing organization for further procedure. The issuing organization at that point will bring the applicant related with that mark sheet no and will request to upload the mark sheet, the issuing organization will combine

1. the share imprinted on applicant's imprint sheet(...Share 2),
2. the authentication key given by the activity searcher or candidate(...Share 3),
3. The share kept at issuing organization's end associated with the mark sheet no, jobseeker provided(...Share 1).

In the event that the decoded picture matches with certificate no(which the certificate issuing organization is having) associated with the mark sheet no.(provided by the job seeker), certificate issuing organization verifies the jobseeker's affirmation to the Portal and if does not Verification gets dropped.

Subsequent to getting a positive impression about the certificate no. the certificate issuing organization checks whether the marks, present as the postfix with the marks matches with the marks, engraved on the mark sheet the jobseeker has transferred.

In the event that the marks coordinate, the certificate issuing organization proclaims that the jobseeker has created a genuine certificate and if does not the issuing organization reports that the jobseeker has delivered a certificate with real certificate no. be that as it may, the marks have been altered.

The message will be passed to the recruiting body through the online entryway. The message can be any of these 3:

1. Jobseeker has produced forged mark sheet(because the unscrambled picture did not coordinate with unique certificate no. associated with the mark sheet no., engraved on mark sheet that the jobseeker has uploaded).
2. Jobseeker has produced mark sheet which produces unique certificate no.(associated with the mark sheet no., engraved on mark sheet that the jobseeker has uploaded), but the marks have been altered.
3. Jobseeker has delivered a bona fide mark sheet.

II. VISUAL CRYPTOGRAPHY

VC coordinates to make shares from the info picture making them contorted so that the yields can converge to remake the first one. The shares are considered as ciphertext. These are matched picture with p pixels. Every one of these pixels is again encoded. Subsequently, n no. of offers can be created by collecting these subpixels. Each offer is a gathering of m high contrast subpixels. These subpixel groupings are regularly square to not curve the point of view the extent of the main picture. Regardless, subpixel groupings that are not square happen in VC estimations and the point of view the extent of the image is balanced properly. This structure can be depicted as an n×m Boolean network S. The structure of S can be delineated subsequently: S = (sij)m×n where sij = 1 or 0 if the jth sub-pixel of the ith offer is dim or white.

The most ordinarily utilized subpixel gathering in VC plan appears in Figure 1. The picture is joined in n shares and the message can be uncovered by consolidating those n shares. The age of the shares depends on the estimation of the pixel and the likelihood of a subpixel gathering happening. The estimation of pixels is either 1(for dark subpixels) or 0(for white subpixels) if the original image was a binary one. A share age plan relating to k=2 and n=2 appears in Figure 1. This is connected to a paired picture by appointing the comparing subpixel gathering to the pixels all through the picture. These outcomes in two irregular shares where the message can't be recognized.

The fundamental method of making shares for 2 out of 2 scheme are white and black pixels are additionally broken down in subpixels. The shares can be of 3 types. These are horizontal, vertical, diagonal to corner shares. These shares are again coordinated to make the no. of offers, required for the reason accordingly. The reconciliation methodology appears in Figure 1.

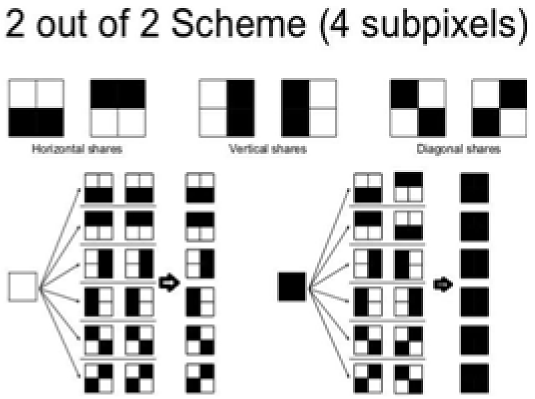


Figure 1

III. VISUAL CRYPTOGRAPHY AND ITS APPLICATION TO SECURE ONLINE CERTIFICATION SYSTEM

There are numerous methodologies and nuts and bolts of dependent on Visual Cryptography. Our methodology in this paper is to recognize forged mark sheet. Here we have attempted to deliver a one of a kind answer to secure the online accreditation framework. Thus the recruiting bodies will almost certainly identify manufactured mark sheet if present.

A. Generating Certificate No.

From the outset, the certificate issuing association will deliver the mark sheet, on which the one of a kind mark sheet no. is generated. That mark sheet no. is likewise imprinted on the mark sheet alongside marks, obtained. After that, a novel certificate no.(associated with that mark sheet no.) is produced which will convey the imprints got as the suffix. In expansion to state this certificate no. will never be uncovered to some other hand(not even the jobseeker or the candidate), will be kept securely at issuing association's hand.

B. Generating the shares and distributing them

Presently, the certificate no. is destructed in 3 shares. Out of these, share 1 is kept at issuing association's end, share 2 will be imprinted on the mark sheet of the jobseeker, share 3 will be given to the activity searcher as an authentication key.

Subsequently in end to this stage neither the authentication no. nor the share 1 will be uncovered to anyone, just certificate issuing organization will keep these two securely.

C. Jobseeker’s certificate verification

From that point onward, when the applicant is supposed to verify his or her certificate as a substantial one to the recruiting bodies, needs to experience a few steps.These are:

Step 1: Jobseeker provides the authentication key and mark sheet to the recruiting body.

Step 2: Recruiting body fetches the online portal with the mark sheet no., printed on the jobseeker's mark sheet for verifying.

Step 3: The online portal brings the certificate issuing organization with the mark sheet no.

Step 4: Certificate issuing organization

i) Fetches the jobseeker associated with the mark sheet no. and asks to upload the mark sheet(for the share 2, imprinted on mark sheet).

ii) Looks for the share 1, kept at their end associated with the mark sheet no.

Step 5: Certificate issuing organization unions share 2(imprinted on marks sheet), validation key (share 3), share 1(kept safe at their end, related with the mark sheet no.).

Step 6: This union unveils a decrypted image.

Step 7: Certificate issuing organization coordinates the decrypted image with the certificate no.(kept secured at their hand only)associated with mark sheet no. of the jobseeker.

Step 8: [From step 7] On the off chance that matches, authentication issuing organization checks whether certificate no. contains the obtained marks(showing on mark sheet, transferred) as postfix or not.

i) If truly, message (a) is that the jobseeker has delivered a total credible testament.

ii) If no, message (b) is that the jobseeker has delivered an authentication with credible certificate no., however, something is unpleasant with the marks, engraved.

Step 9: [From step 7]If that the certificate no.(issuing body having)associated with the mark sheet no. does not coordinate with the unscrambled picture

Message(c) is that the jobseeker has delivered a fabricated mark sheet.

Step 10: This message will be passed to the online portal from certificate issuing organization's end.

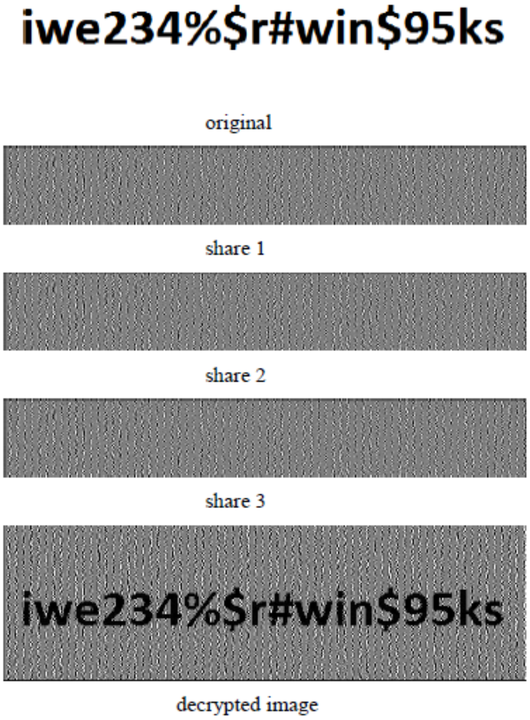
Step 11: The recruiting body will get feedback about the jobseeker through the online. Message can be any of these 3 i) message (a), ii) message (b), iii) message (c) accordingly.

The flowchart of the entire method is expressed to sum things up in figure 2.

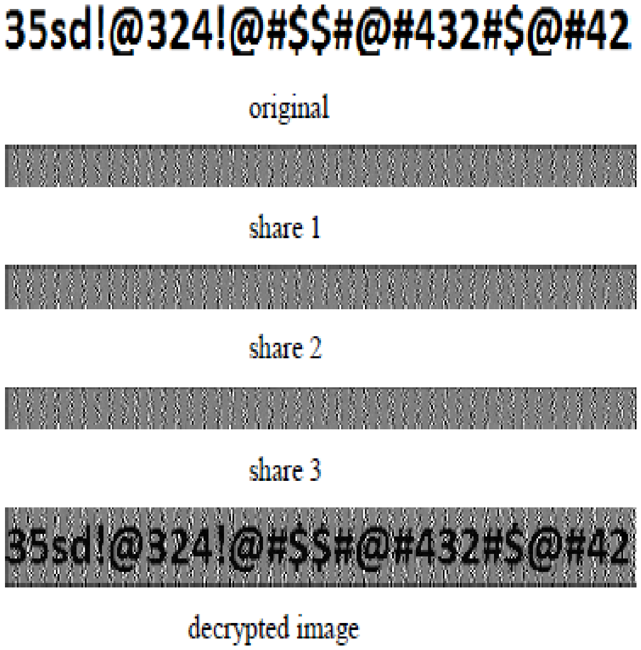
IV. RESULT AND IMPLEMENTATION OF VC FOR DETECTING FORGED MARKSHEET

A few pictures of numbers are appeared beneath alongside their 3 shares and the unscrambled picture.

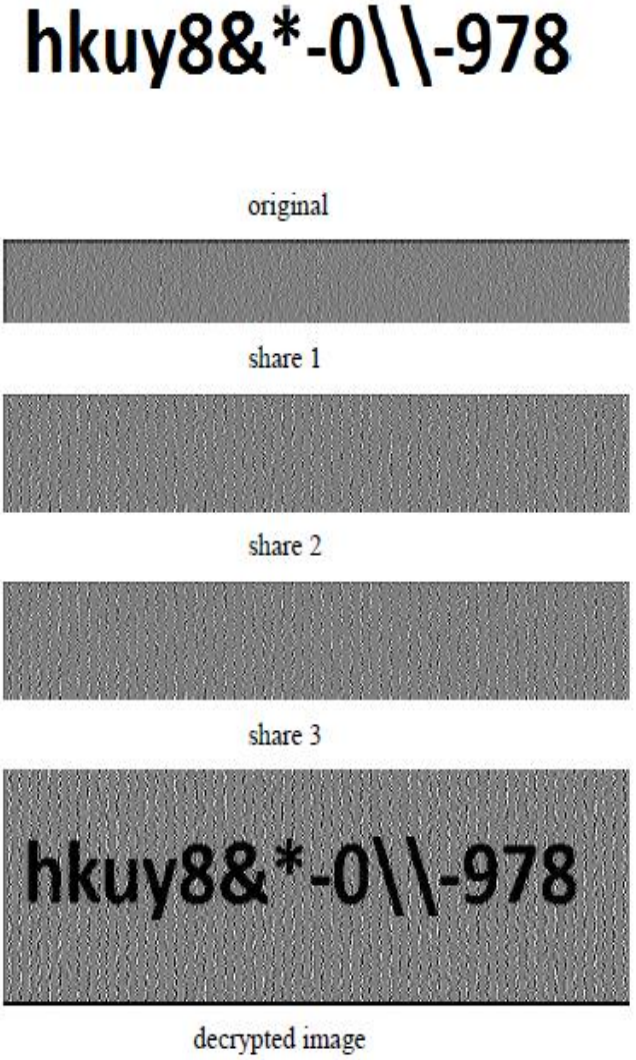
1. Picture 1



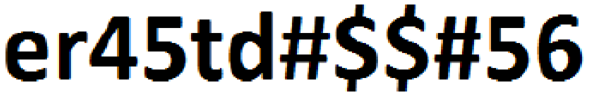
2. Picture 2



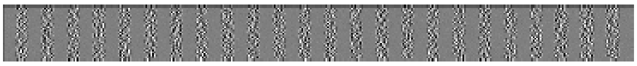
3. Picture



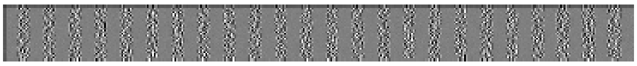
4. Picture



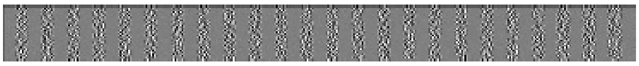
original



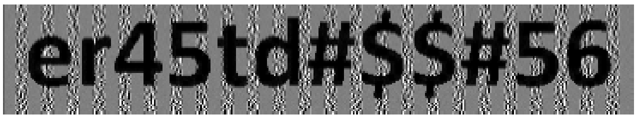
share 1



share 2

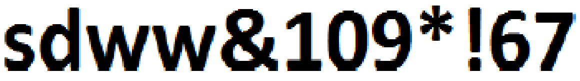


share 3

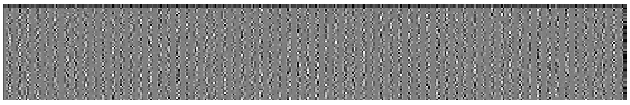


decrypted image

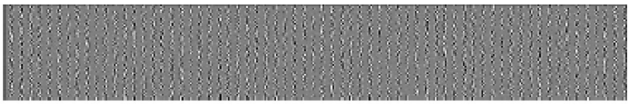
5. Picture



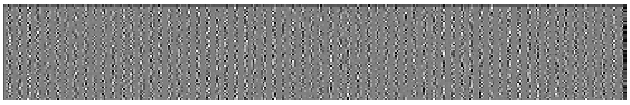
original



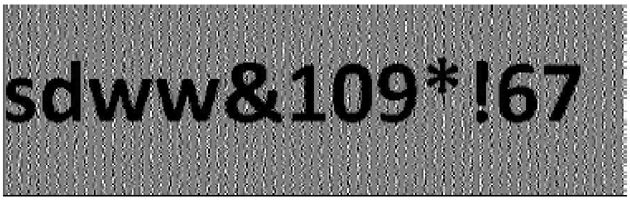
share 1



share 2



share 3



decrypted image

V. CONCLUSION

This paper proposed a novel scheme to detect fraud certificates in a low cost efficient way. By generating shares which are kept by different stakeholders, the procedure ensures unpenetrable security. As visual cryptography is being used for generating shares, mathematically decrypting them to get hold of the key is impossible. In this way the architecture gurantees a better solution of the fake certificate problem than any other cryptography sceme.

REFERENCES

1. Visual Cryptography(Moni Naor*and Adi Shamir)[Department of Applied Math and Computer Science, Weizmann Institute, Rehovot 76100, Israel.]
2. Implementation K out of N Visual Cryptography using K out of K Scheme (Abul Hasnat, Dibyendu Barman ,Government College of Engineering & Textile Technology Berhampore, West Bengal, India)(Satyendra Nath Mandal Kalyani Government Engineering College Kalyani, West Bengal, India)
3. Generalized Graph- based Visual Secret Sharing Schemes for Multiple Secrets (Yuji Suga suga@iij.ad.jp ,Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi Chiyoda-ku, Tokyo 102-0071, Japan)
4. Visual Secret Sharing Scheme With (k, n) Threshold Based on QR Codes (Song Wan, Yuliang Lu, Xuehu Yan and Lintao Liu ,Hefei Electronic Engineering Institute ,Hefei, China)
5. EXTENDED VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGES WITH NO PIXEL EXPANSION(Xiaoyu Wu, Duncan S. Wong and Qing Li ,Department of Computer Science, City University of Hong Kong, Tat Chee Avenue, Hong Kong, China)
6. PUF Authentication using Visual Secret Sharing Scheme(Devarapalli Naveen ,TIFAC-CORE in Cyber Security,Amrita School of Engineering, Coimbatore,Amrita Vishwa Vidyapeetham, India)(Praveen K ,TIFAC-CORE in Cyber Security,Amrita School of Engineering, Coimbatore,Amrita School of Engineering, Coimbatore)
7. Cheating prevention visual cryptography scheme using Latin square(Yawei Ren1,2,3 , Feng Liu1,3, Teng Guo4, Rongquan Feng5, Dongdai Lin1 ;1State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, People's Republic of China 2School of Information Management, Beijing Information Science and Technology University, Beijing 100192, People's Republic of China 3University of Chinese Academy of Sciences, Chinese Academy of Sciences, Beijing 100190, People's Republic of China 4School of Information Science and Technology, University of International Relations, Beijing 100091, People's Republic of China 5School of Mathematical Sciences, Peking University, Beijing 100871, People's Republic of China)
8. k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence (Shyamalendu Kandar Department of Computer Sc. & Engineering Haldia Institute of Technology Haldia, India)(Bibhas Chandra Dhara Department of Information Technology Jadavpur University Kolkata, India)

AUTHORS PROFILE

Mr. Tridib Chakraborty, Asst Prof, Dept of Information Technology , Guru Nanak Institute of Technology has completed BTECH in Information Technology) ,under WBUT (presently MAKAUT), M.E. from JU, Kolkata and currently pursuing research in areas of Cryptography, Data Security, Neural Networks. E-mail: tridib.chakraborty@gnit.ac.in

Mr. Sudeep Ghosh, Assistant Professor, Dept of Information Technology, Guru Nanak Institute of Technology, has completed B.Tech in Information Technology, from WBUT (presently MAKAUT) in year of 2008, and M.E. in Information Technology from Indian Institute of Engineering Science & Technology, Shibpur (IIEST) in the year of 2011. He is currently pursuing PhD from Indian Institute of Information Technology, Kalyani. He is life time Associates Member of Institute of Engineers (IE). He has more than eight years of academic experience as an Assistant Professor and his current research interests includes Classical Cryptography, Cloud Security, Information Security. E-mail: sudeep.ghosh@gnit.ac.in

Mrs. Trishita Ghosh, Asst Prof, Dept of IT , Guru Nanak Institute of Technology has completed BTECH in Information Technology) ,from UIT, M.Tech. from CU, Kolkata . She is currently pursuing research in areas of Mobile Computing, VANET. E-mail: trishita.ghosh@gnit.ac.in

Miss. Suparna Karmakar, Asst Prof, Dept of IT , Guru Nanak Institute of Technology has completed BTECH in Information Technology) ,under WBUT (presently MAKAUT), M TECH(MSS) from NITTTR, Kolkata and currently pursuing Ph.D. from IIIT, Kalyani. **Research Area:** Data Science, Petri Net Modeling Tool. E-mail: Suparna.karmakar@gnit.ac.in

Name: Chowdhury Md Mizan
Designation: Assistant Professor
Qualification: BTECH (CSE) Narula Institute Of Technology, under WBUT (currently MAKAUT)**,** M TECH(IT) from University Of Calcutta, Kolkata**,** Ph. D.(pursuing) from Techno India University, Salt Lake Sec V,Kolkata **Research Area:** Multi biometrics,Fingerprint Recognition
Subjects: Operating System(IT503),Internet Technology(IT702A)
E-mail: chowdhurymd.mizan@gnit.ac.in