International Journal of Management, IT & Engineering
Vol. 8 Issue 11, November 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CHANGING TRENDS IN CAPTCHA BREAKING MECHANISMS FOR GRAPHICAL TEXT BASED CAPTCHA

Mir Aman Sheheryar*

Abstract—

CAPTCHA determines difference between human and machine. Thus is widely used for Web programs over Internet. It is the security entrance and provides permission of access when it tests credentials depending upon its need. The versatility of CAPTCHA depends upon its firmness to withstand attacks. Better CAPTCHA's are more secure for implementation. To breach the security mechanism provided by CAPTCHA it needs to be break in order to achieve intrusion. Breaking CAPTCHA involves number of mechanisms which when fallowed properly acquire quality result. In this research procure we presented the various breaking mechanism on Graphical text based CAPTCHA which are categorised under five stages and touted out the analysis on the basis of these approaches. We have recollected various mechanisms used up in breaking text based graphical CAPTCHA.

Keywords—Intrusion,Automated Bots, Turning Test, HIP, *Artificial Intelligence.*

* **Department of Information Technology, Central University of Kashmir, Srinagar, India**

I. INTRODUCTION

CAPTCHA is the strong security mechanism placed for web Applications after password. Password provides only authentication for application access whereas CAPTCHA has evolved as an authorative to discriminate between Human and Machine. CAPTCHA an acronym for "Completely Automated Public Turning Test To Tell Computer and Humans Apart"[1]. CAPTACH works on "Turning Test" that use HIP" Human Interactive Proof"[2]. In turning test series of user is provided with task to complete and upon completion of task user is ascertained if task is cleared by user further access is availed and it is judged that user is human, But in case of failure user is denied access and he is judged to be machine. Turning test provides only tasks and HIP differentiate legitimate user. When legitimate user clears the task at that time it is clear that user is human and in case of failure user is machine. With the introduction of CAPTCHA it offered compact security for various types of web applications enjoyed over web. With the handy CAPTCHA mechanism in hand, yet it faces tuff time to defend against breaking attempt under the influence of breaking mechanism involving machine like bots. With every breaking attempt performed on CAPTCHA its security parameters are tested, so as to stand in all odds. CAPTCHA is the obtained outcome of "Artificial Intelligence" that relies on human computer interaction "HCI" where interaction between computer and human is achieved in best possible manner. The approach performed to implement HCI is chosen so wisely that it becomes convenient for novel human use. With vast research being conducted in the field of security, enough work on CAPTCHA security mechanism is available and progress is achieved continuously. We have reviewed various Breaking Mechanisms in the field of Graphical Text Based CAPTCHA and presented them in coherent orientation so as to provide precise approach for users for adopting breaking mechanism procedure to intrude CAPTCHA, thus negating the determination of user being machine or human.

Section I contains the introduction of CAPTCHA security mechanism and need for CAPTCHA, Section II contain the related work of Breaking mechanism for CAPTCHA with changing trends due to advancement in technology same is produced under five stages of processing in this pursuer ,Section III contains complexity criteria where various issues have been pointed out that are faced during Breaking mechanism . Section IV Comparative analysis where matching

performance and correlation of different research pursuers have been touted out. Finally Section V contains the conclusion and Future scope followed by Acknowledgment recommendations.

II. RELATED WORK

Vast research is present on breaking mechanism of CAPTCHA. In order to choose a good CAPTCHA breaking mechanism it is mandatory to investigate the existing mechanisms for advantages/drawbacks of existing CAPTCHA breaking schemes on parameters like time complexity, strength, interference, misrepresentation and technology used to obtained required outcome. Various techniques have evolved over the growing years to break CAPTCHA consuming less effort. At "Carnegie Mellon University" for commercial scenario in 2000 Captcha was introduced to provide security to 'Yahoo Chat room'. After the introduction of CAPTCHA at the same time its breaking mechanism came into being for testifying the security offered by CAPTCHA. Table 1 provide summed up CAPTCHA breaking mechanism.

Protection mechanism in CAPTCHA

The main ability of CAPTCHA lies on the amount of resistance it shows against the attacks performed on it. Distorted appearance form the main feature of Graphical Text Based CAPTCHA fallowed by number of transitions like.

- Vast set of characters including digits, English/ native alphabets, special symbols and characters.
- Tightly coupled character set, of varying length. That increases the level of resistance to withstand dictionary based attack.
- Wise colour selection as to confuse attacker against recognition.

For making sound CAPTCHA mechanism above standard steps form bedrock and in order to intrude through CAPTCHA mechanism it need to be cracked to achieve successful result.

The same is put forth in different research pursuers that are discussed in five stage manner.

Time attacks were testified in [3], the authors examined the strength, frequency and explained detailed procedure to enhance the quality of strength and frequency.

Stage 1: PREPROCESSING STAGE

It is the initial stage where from CAPTCHA intrusion begins. Here CAPTCHA is explored so as to figure out its loopholes for cordial evade before performing segmentation, recognition procedure. In Preprocessing stage Binarization, thinning and Denoising of CAPTCHA is done in order to achieve cordial solution

.

Binarization of CAPTCHA

Here CAPTCHA is selected to remove background distortion. CAPTCHA is analysed for global threshold. sauvola[4] and otsu's used dynamic threshold for their procedure.

Thinning of CAPTCHA

In thinning procedure boundary of CAPTCHA is selected for easy processing. In this CAPTCHA is subjected to Non iterative and iterative algorithm like Hilditch algorithm, zhang and suen algorithm in[5,6]. Character distance shall remain same before and after thinning procedure.

Denoising of CAPTCHA

In this procedure feasible technique is considered for noise removal. Noise is there for distortion to make CAPTCHA breaking difficult. Noise also appears as an outcome of Binarization. Domain spatial, Gibbs and Hough transform, morphology removal procedure, attached components procedure, wavelet transformation are different techniques for removing noise.

s.no	Stage	Procedures
1	**PREPROCESSING STAGE**	• Binarization of Captcha • Thinning of CAPTCHA • Denoising of Captcha
2	**SEGMENTATION STAGE**	**Segmentation on Individual characters** • *Character projection Segmentation* • *Connected components segmentation* • *Character width segmentation* • *Character attributes segmentation* • *Contour segmentation:* **Segmentation on character outline** • *Structure segmentation:* • *Filter segmentation:*
3	**COMPOSITE STAGE**	• Repetition • Non- Repetition
4	**RECOGNITION STAGE**	**Template Recognition** • *Traverse Scanning Recognition* • *Parallel Local feature Recognition* **Characteristic Recognition** • *Structure Attribute Recognition* • *Analytical recognition* **Expert System Recognition** • *Neural Network Recognition* • *Conventional Recognition* • *Deep Learning Recognition*
5	**POST-PROCESSING**	• Election Post-Processing. • Rejection Post-Processing

Table 1: CAPTCHA Breaking Mechanism

Stage2: SEGMENTATION STAGE

When it comes to break Graphical text based CAPTCHA. Segmentation procedure and non-segmentation procedure are employed to explore the vulnerabilities of CAPTCHA in order to attain soft Bypass and in most of the scenarios it proved handy to break installed security offered by CAPTCHA. The procedure of segmentation is employed in step wise scheme which is based on nature of CAPTCHA. The prime analysis is done on the basis of Gap between characters[7], adjoined region[8], vertical projection[9], and calculation is done by judging misrepresentation evaluation[7], pixel character statics[9] and SVM as discussed in[10].

Segmentation procedure is employed by categorizing whole procedure under two schemes which interim also use their prescribed modules and procedures. the main segmentation procedures are(i) segmentation on individual character, (ii) segmentation on character outline.

2.1 Segmentation on Individual characters:

Segmentation is performed on CAPTCHA in order to separate characters from each other in CAPTCHA string. Segmentation is followed by character projection, connected components procedure. We can also make use of procedures like character width, character attribute and character boundary.

2.1.1 Character projection Segmentation:

Determination of feasible plane is analysed among localized character pixels under various scenario. It is applicable to find tightly coupled or loosely coupled characters. When elaborated further this procedure involve vertical projection guideline, horizontal projection guideline segmentation as discussed by researchers in[1].

2.1.2 Connected components segmentation:

In connected component segmentation adjacent placed characters are investigated for slant, angle, skewness and tight placements. In tight placements characters allowing character in the form of set for processing did not provide handy result. Researchers acquire 90% of success in[11] on MSN CAPTCHA involving connected components and vertical projection. Their work revolve around dividing the CAPTCHA string and obtain characters in the block form having

different colours and proved vertical projection solution as handy as their outcome during research.

2.1.3 Character width segmentation:

Width segmentation is employed when CAPTCHA image is analysed as whole. Varying width is used to segment CAPTCHA as performed in[12], varying width for segmentation divide character segmented into recognition outcome . The recognized outcome is categorised under four pattern of recognised set for solution. Width range among character was taken as regular. Dynamic programing for attaining feasible output segmentation by considering minimum and maximum width were employed in[10] thus bypassing the use of regular character width for attaining result.

2.1.4 Character attributes segmentation:

CAPTCHA attributes are determined by internal and external attributes for string. Inside attribute grouping was done in[13] involving internal attribute. For determining outside attribute researchers in[14] produced " middle axis point separation algorithm" for CAPTCA. Where for segmentation points, central pixel are used in back between two disarticulate object pixel.

.2.1.5 Contour segmentation:

To figure out contour line of CAPTCHA Character set. Contour based segmentation is used to determine CAPTCHA contour as performed in[15] where researchers took confidence interval into consideration.

2.2 Segmentation on character outline:

Segmentation on character outline stressed on various characters than that of individual. Segmentation on character outline uses structure segmentation and filter segmentation.

*2.2.1 Structure segmentation:*Structure segmentation involve dividing the CAPTCHA image into small black and white area components, firstly black area is located and then white area is located so as to localize the shared area for easy identification as explored in[17]

2.2.2 Filter segmentation:

Filter segmentation use "Gabor Filter" as firstly produced in[17]. In Filter segmentation CAPTCHA is divided into four scenarios by performing the image processing convolution.

Stage3: COMPOSITE STAGE

In Composite stage summing up of individual character chunk is performed for recognition. Composite stage comprises of two procedures used for breaking repetition and Non-repetition.

3.1 Repetition:

In repetition characters obtained and character created by possible choice are large than true character as discussed in[17]. For the determination of every character is named from right, left, up and down.

3.2 Non-repetition:

In the non-reputation character obtained and created using possible choice corresponds among one another. If in this case non-repetition is attained overlap stroke movement as used in[18] are employed to build full character

Stage 4: RECOGNITION STAGE

The recognition is attained upon subjecting the CAPTCHA to the following schemes for recognition that are Template, characteristic and Expert system recognition. Further these three schemes involve fragmented procedures that assist in recognition.

4.1 Template Recognition

In template recognition matching of similarity is done using global property and local attributes. Maximum similarity among pixel characters is matched and acquired in order to have handy recognition.

4.1.1 Traverse Scanning Recognition

In traverse scanning recognition method correlation computation and region comparison are performed to get similarity. Before obtaining final outcome rough matching is gathered and after that accurate gathering is done as performed in[19].

4.1.2 Parallel Local feature Recognition

Here point set attribute is used for image comparison. Malik in[20] discussed procedural way to achieve breaking by using local feature recognition on Gimpy and Ez gimpy. Parallel local feature recognition is good when Shape Matching and Facial Recognition need to be done.

4.2 Characteristic Recognition

The ability of Characteristic Recognition lies on the demography of character formation in CAPTCHA image. Breaking can be done by exploiting the demographic behaviour of character. It uses Structure Attribute and Analytical recognition scheme to perform Characteristic recognition.

4.2.1 Structure Attribute Recognition

In structural Attribute Recognition emphasis is laid down over the physical demography of the character for determining "Escalation point", "Concave loops and convex loops. In[21] researchers breached the Yahoo CAPTCHA using structure Attribute Recognition for determining the bound loops and direction.

4.2.2 Analytical recognition

Analytical recognition uses Raw Snare feature, Projection feature and boundary features to approach problem. Analytical recognition bypass presence of noise as discussed in[9] where researchers breaked Captchaservice.org with ~100% success.

4.3 Expert System Recognition

The Expert system use less human intervention as that of non-expert systems. Here series of iterations are performed to obtain suitable outcome. Purpose based algorithms are best employed to acquire feasible output. Neural network recognition, Deep Learning recognition and

Convolution recognition are procedural ways of using expert system recognition for breaking CAPTCHA.

4.3.1 Neural Network Recognition

Neural network recognition is good for breaking CAPTCHA because of its intelligent ability. Repeated training of network is done so as to train system for further processing. Working of neural network is an analogy to human neuron. Precession of 53.3% and 27,52% were achieved in[22] by researchers using Back propagation Neural Network and Cross Entropy for Taboo, eBay and MSN CAPTCHA sets.

4.3.2 Conventional Recognition

In convolution recognition KNN and SVM classifiers are used to find closest neighbour. KNN provide good success percentage as compared to CNN, SVM and is lazy than CNN as discussed in[17]. Using hyperplane separability can be determined by SVM. Where Kernel function matches true feature in Non Linear order having vast freedom. "SIGMOID, LINEAR, POLY and RBF" were used to perform comparison of Kernel functions in[10].

.3.3 Deep Learning Recognition

Deep learning recognition gives handy result in breaking CAPTCHA using RNN, CNN, LSTM-RNN. Efficient accuracy for CNN was justified practically in[2,11,16,13] avoiding feature extraction process.

Stage 5: POST-PROCESSING.

Post processing enhances the outcome from previous stages. This procedure uses Election Post-processing and Rejection Post Processing.

5 .1 Election Post-Processing

Election Post-Processing uses neighbourhood optimization and total optimization. In neighbourhood optimization confidence interval is considered for discrete character. The high confidence interval is, more accurate the character will be. For good accuracy characters with

high confidence level are selected as in[23]. Traverse graph for overall optimization and dynamic programming for precise result were used in[4,10,17] by researcher.

5.2 Rejection Post-Processing

Rejection post- processing is used to vindicate that the test samples contemplate the training set examined for recognition. Rejection post processing provide efficient CAPTCHA recognition. Multiple feature, confidence interval, last character, string distance and string distance were explored in [22]. Apart from this not much work present show the use of Rejection Post-Processing

Complexity creteria

The prime research problems in the field of CAPTCHA arise in terms of its complexity that is generalised under following problems as database construction for testing, Segmentation –free problem of CAPTCHA recognition Assorted CAPTCHA recognition, Pertinence deep learning modal, declination of Text based CAPCTAH and Confusable characters leading Misrecognition

1. *Database construction for testing.* In order to work upon CAPTCHA there needs to be proper generation of CAPTCHA using software or online available CAPTCHA can be employed for getting results after processing. Acquiring CAPTCHA using generation or online availability led to disproportionation analytical parameters. So in order to maintain uniformity for testing invoking machine learning there should be proper construction of common available Database that shall be used in research pursuers for training system.

2. Assorted CAPTCHA recognition. To achieve coherent recognition test and training set should be of same type. But CAPTCHA characters show varying change depending upon the type of CAPTCHA. In order to overcome this scenario our classifier radically should be capable enough to tackle Assorted recognition. So classifiers have to be wisely designed.

3. Segmentation-Free problem of CAPTCHA Recognition. To segment a CAPTCHA is an old problem from preceding years. But with growing technology the process of segmentation achieve high success for individual character segmentation. Yet CAPTCHA have not been fully breaked and calculated outcome is less. This problem need to addressed as CAPTCHA string is

based on CCT. In order to solve this problem researchers are hope full to make technical use of Deep learning.

4. *Pertinence Deep learning strategy.* The current deep learning strategies like CNN,RNN,DRL,LSTM,BLSTM,MDLSTM used in the field of Breaking CAPTCHA were not soundly employed to tackle CAPTCHA efficiently, but with further enrichment to Deep learning strategies a colossal modal can emerge to handle this scenario.

5. *Rejection of Text Based CAPTCHA.* The field of Rejection has a vast potential for researchers as it is not much known. Day by day changing scenarios led to the innovation of more precise recognition techniques. With more precession we can ensure good rejection.

6. *Confusable characters leading Misrecognition.* The character intermixing in CAPTCHA involve presence of confusable characters like 'm' and 'nn', 'w' and 'vv' etc that leads to misrecognition rate. For exact feature extraction using deep learning the recognition rate of confusable character can be increased by repeated training methods in deep learning.

III. COMPARATIVE ANALYSIS

Here we have compared various procedure in terms of versatility, applications and constrains for segmentation and recognition schemes. Comparison of segmentation and recognition procedures for CAPTCHA breaking mechanisms can be figured out from the table2 for Segmentation and

Table 2: Segmentation Comparison.

Segmentation Approach	Approach employed	Adherence	Tilt	Distortion	Overlap	Description
Individual character	*Projection*	**Yes**	**No**	**No**	**No**	**Overlapped**
	Connected Components	**No**	**Yes**	**Yes**	**No**	**Limited**
	Width	**Yes**	**No**	**No**	**No**	**overlapping**
	Feature	**Yes**	**No**	**No**	**No**	**Sever distort**
	Boundary	**Yes**	**yes**	**Yes**	**No**	**Notable**
Individual Component	*Structure*	**Yes**	**Yes**	**Yes**	**Yes**	**Easy to segment**
	Filter	**Yes**	**Yes**	**yes**	**Yes**	**Complex**

Table 3: Recognition comparison.

Recognition Approach	Feature	Algorithm	Advantages	Limitations
Template Matching	*Global optimization* *Local features*	**Travers search** **Shape Context**	• Simple • Robust for Image scaling and Affine transformation	• Require large library • Rotation invariant.
Character Feature	*Structure Feature* *Analytical Feature*	**Character Structure** **Analytical Feature**	• Detail sensitive. • Withstand noise interference.	• Application limited. • Distortion is high for noise interference
Expert system	*Template* *Conventional* *Deep learning*	**SVM,KNN** **BPNN,CNN** **CNN,RNN,LSTM-RNN**	• Better Adaptability • Flexible structural design. • High recognition accuracy • Prevent gradient using time memory function.	• Limited to infinite samples. • Computational complexity. • Slow convergence rate. • Disappear time gradient • Inability of attribute extraction automatically.

Researchers in[24] have explored strength and weakness of Graphical Text Based CAPTCHA same is summed up in tabular form in table 4.

Table4: Strength and Weakness of Graphical Text Based CAPTCHA System as discussed in [24]

CAPTCHA	Strength	Weakness	Drawbacks
Graphical Text based	1. Distorted text image is presented for the test to user. 2. Hollow, 3D, Opaque appearance of Text Image. 3. Tilt, skewness and deformation. 4. Similar background and foreground Colour.	1. High distortion makes it difficult for humans to read CAPTCHA Clearly. 2. Modern OCR's algorithms can achieve over 90% success in cracking.	1. In text images, user has some problem to identify the correct text or characters. 2. Multiple fonts. 3. Font size. 4. Blurred Letters 5. Wave Motion. 6. Amount of Noise

Figure 1 show the graphical result obtained after subjecting Chaac-CAPTCHA'H against cracking in[25].It with stands cracking as compared to already existing CAPTCHA's that include Gimpy, Ez-Gimpy, Secure image, Cryptography, Megaupload. There work gave new CAPTCHA known as "Chaac-CAPTCHA" in two variants Easy and Hard variant
and after experimental verification and calculation hard variant show 99% success rate to withstand cracking.

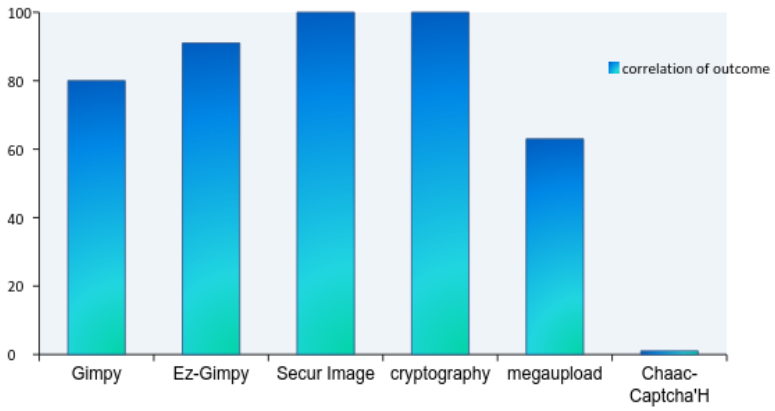

Figure 1: Result obtained in [25] showing Chaac-H withstand cracking Attack.

IV. CONCLUSION AND FUTURE SCOPE

We have produced the insight of changing trend in CAPTCHA breaking mechanism for Graphical Text based CAPTCHA.

With the introduction the need and requirement of CAPTCHA has been discussed along with the Breaking mechanism. With relevant literature survey we figured out the five stage procedure for breaking Graphical Text Based CAPTCHA as Pre-Processing, Segmentation, Composite, recognition and post –Processing stages. After that we discussed the complexity criteria in which insight is provided for various issues faced while dealing with the breaking mechanism fallowed comparative analysis regarding segmentation mechanism and recognition mechanism based upon features, algorithms, and advantages and limitations. Keeping in view the detail investigation for CAPTCHA Breaking Mechanism we will be looking further to propose the Recognition Engine/ Analytical Engine, that shall be efficient to Break CAPTCHA under different circumstances.

ACKNOWLEDGMENT

For motivation, much recommended direction and moral for this pursuer. Highly thankful to Er. Zahoor Ahmed Najar and Dr Saleem Parveiz Mir.

.

REFERENCES

[1] L. Von Ahn, M. Blum, and J. Langford, “Telling humans and computers apart automatically”, Communications of the ACM, vol. 47, no. 2, pp. 56.60, 2004.

[2] K. Chellapilla and P. Y. Simard, ¡°Using Machine Learning to Break Visual Human Interaction Proofs (HIPs), in Proceedings of the Advances in Neural Information Processing Systems, pp. 265.272, of Advances in Neural Information Processing Systems, 2004.

[3] N. Roshanbin and J. Miller, “A survey and analysis of current CAPTCHA approaches”, Journal of Web Engineering, vol. 12, no. 1-2, pp. 001.040, 2013.

[4] J. Sauvola and M. Pietiainen, “Adaptive document image binarization”, Pattern Recognition, vol. 33, no. 2, pp. 225.236,2000.

[5] C. J. Hilditch, “Linear Skeletons from Square Cupboards”, Machine Intelligence, pp. 403.420, 1969.

[6] T. Y. Zhang and C. Y. Suen, "A fast parallel algorithm for thinning digital patterns", Communications of the ACM, vol. 27, no. 3, pp. 236.239, 1984.

[7] G.Moy,N. Jones, C.Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs", in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2004, pp. II23.II28, July 2004.

[8] A. Bansal, D. Garg, and A. Gupta, ¡°Breaking a Visual CAPTCHA: A Novel Approach usingHMM,2008,https://pdfs.semanticscholar.org/3c2c/9af1e9a3b7095edaf8f205dfbadc30f 917fb.pdf.

[9] J. Yan and A. S. El Ahmad, "Breaking visual CAPTCHAs with pattern recognition algorithms", in Proceedings of the 23rd Annual Computer Security Applications Conference, ACSAC 2007, pp. 279.291, December 2007.

[10] F. Jean-Baptiste and R. Paucher, ¡°The Captchacker Project,2009, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1 .1.800.3065&rep=rep1&type=pdf.

[11] J. Yan and A. S. E. Ahmad, "A low-cost attack on a Microsoft Captcha", in Proceedings of the 15th ACM conference on Computer and Communications Security, CCS 08, pp. 543.554,USA, October 2008.

[12] C. Hong, B. Lopez-Pineda, K. Rajendran, and A. Recasens, "Breaking Microsofts Captcha", 2015, https://courses.csail.mit.edu/6.857/2016/files/hong-lopezpineda-rajendran-recansens.pdf.

[13] A. S. E. Ahmad, J. Yan, and M. Tayara, "The Robustness of GoogleCAPTCHAs", Computing Science Technical Report CSTR-1278, Newcastle University, 2011.

[14] S.-Y. Huang, Y.-K. Lee, G. Bell, and Z.-H. Ou, "An efficient segmentation algorithm for CAPTCHAs with line cluttering and character warping", Multimedia Tools and Applications, vol.48, no. 2, pp. 267.289, 2010.

[15] R. A. Nachar, E. Inaty, P. J. Bonnin, and Y. Alayli, "Breaking down Captcha using edge corners and fuzzy logic segmentation/ recognition technique", Security and Communication Networks, vol. 8, no. 18, pp. 3995.4012, 2015.

[16] A. S. El Ahmad, J. Yan, and L. Marshall, "The robustness of a new Captcha", in Proceedings of the 3rd European Workshop on System Security, EUROSEC¡¯10, pp. 36.41,April 2010.

[17] H. Gao, J. Yan, F. Cao et al., "A Simple Generic Attack on Text Captchas", in Proceedings of the Network and Distributed System Security Symposium, pp. 1.14, San Diego, Calif, USA, 2016.

[18] B. B. Zhu, J. Yan, Q. Li et al., "Attacks and design of image recognition CAPTCHAs", in Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS10,pp. 187.200, October 2010.

[19] F. Dai, H. Gao, and D. Liu, "Breaking CAPTCHAs with second template matching and BP neural network algorithms", International Journal of Information Processing and Management, vol. 4, no. 3, pp. 126.133, 2013.

[20] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: breaking a visual Captcha", in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 1, pp. 134.144, June 2003.

[21] H. Gao, W. Wang, Y. Fan, J. Qi, and X. Liu, "The robustness of connecting characters together CAPTCHAs", Journal of Information Science and Engineering, vol. 30, no. 2, pp. 347.369, 2014.

[22] L. Zhang, L. Zhang, S.-G. Huang, and Z.-X. Shi, "A highly reliable CAPTCHA recognition algorithm based on rejection",Acta Automatica Sinica, vol. 37, no. 7, pp. 891.900, 2011.

[23] C. Hong, B. Lopez-Pineda, K. Rajendran, and A. Recasens,"Breaking Microsoft's CAPTCHA," 2015, https://courses.csail.mit.edu/6.857/2016/files/hong-lopezpineda-rajendran-recansens.pdf.

[24] Mir Aman Sheheryar, P. k Mishra and A. K Sahoo, "A REVIEW ON CAPTCHA GENERATION AND EVALUATION TECHNIQUES", ARPN Journal of Engineering and Applied Sciences, VOL. 11, NO. 9, MAY 2016

[25] Mir Aman Sheheryar, A. K Sahoo, "Chaac -Captcha: An Improvisation of Graphical based Captcha with Dynamic Random Misrepresentation for Discrimination Between Human and Machine", International Journal of Engineering Research & Technology (IJERT), Vol. 6 Issue 05, May - 2017

.