International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:9, 2009

Unified Method to Block Pornographic Images in Websites

Sakthi Priya Balaji R., and Vijayendar G.

***Abstract*—**This paper proposes a technique to block adult images displayed in websites. The filter is designed so as to perform even in exceptional cases such as, where face detection is not possible or improper face visibility. This is achieved by using an alternative phase to extract the MFC (Most Frequent Color) from the Human Body regions estimated using a biometric of anthropometric distances between fixed rigidly connected body locations. The logical results generated can be protected from overriding by a firewall or intrusion, by encrypting the result in a SSH data packet.

***Keywords*—**Face detection; characteristics extraction and classification; Component based shape analysis and classification; open source SSH V2 protocol.

I. Introduction

THERE is a need for a good filter that can block adult images alone and not other non-objectionable data distributed through websites. Unlike other image processing systems, this system has to work considering certain real time factors wherein the target is the object in the image, which is content of nudity.

The target object may vary with color, pose and illumination criterions. Most methods use Face Detection as the first step in the process of detecting adult images. These methods fail, when face is not visible in the image. Hence, to overcome this drawback, our paper suggests the integration of the results of Face Detection, Shape Analysis and lexical analysis of the web page to form a unified logical result. Also to increase precision we suggest processing the image after separating it into R, G, B and Negative channels. The generated result can be a cipher text that is secured using SSH protocol.

II. Basic Procedures

Phase I of the system attempts to recognize the faces in the image. If face recognition is successful, then the skin color is extracted from the facial regions. The extracted skin information is compared with the skin like colors stored in the color database. Further comparing the same image after separating them into channels including Negative, enhances the precision in comparison. When the test colors are negated, shades of different colors can be restricted to a single color. [Orange, red, brown are reduced to shades of blue after negation. If face recognition is unsuccessful, the system moves to Phase ii where the system performs Pose Estimation of Human Like objects and extracts the MFC (Most Frequent Color) and repeats the rest of the processes, as done by phase I.

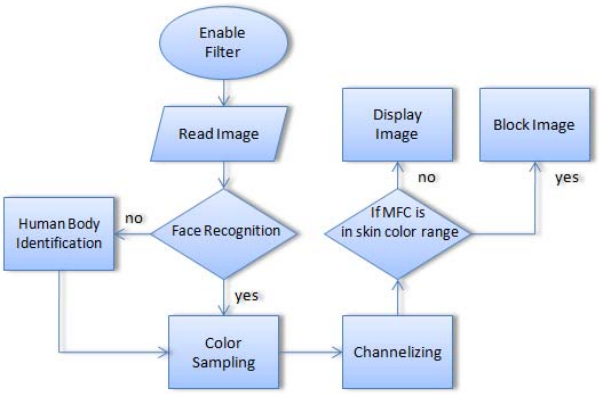

Fig. 1 Basic Layout

A. Face Recognition

The face recognition algorithm used in this system treats faces as three-dimensional surfaces. It is therefore necessary to obtain first the facial surface of the subject. Here, the focus is on methods that produce the surface gradient (∇z) and the construction of the actual surface is not necessary, thereby reducing computational effort and reducing numerical errors. The values of the surface gradient (∇z) can be obtained from a photometric stereo.

B. Photometric Stereo

The photometric stereo technique [8] consists of obtaining several pictures of the same subject in different illumination conditions and extracting the 3D geometry by assuming a Lambertian reflection model. It is assumed that the facial surface is represented as a function, is viewed from a given position along the z-axis. The object is illuminated by a source of parallel rays directed along li. We assume a Lambertian reflection model, i.e. the observed image is given by,

$$Ii(x,y)=\rho(x,y)n(x,y).li, \quad (1)$$

Where $\rho(x,y)$ is the object albedo, and $n(x,y)$ is the normal to the object surface. Using matrix-vector notation, (1) can be rewritten as

$$I(x,y)=Lv \quad (2)$$

Given at least 3 linearly independent illuminations and the corresponding observations, one can reconstruct the values by point wise least-squares solution.

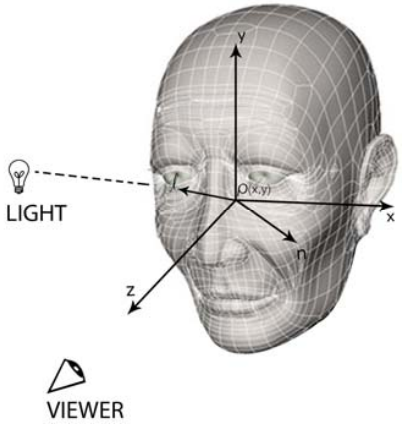

Fig. 2 Photometric stereo acquisition scheme

When needed, the surface can be reconstructed by solving the Poisson equation with respect to ∇z. In this work, we adopt the photometric stereo approach due to its simplicity.

C. Human Identification using Body Shape

When the Face Recognition fails, an alternative method has to be used to make logical decisions. For these purposestatic anthropometric distances [7] is utilized, as a biometric for human identification. The 3D landmark data from the CAESAR database is used to form a biometric consisting of distances between fixed rigidly connected body locations. This biometric is explicit, and invariant to view and body posture. This technique is used to compute the irregularity of human bodies, and to distinguish the interpersonal and intrapersonal distance distributions. The former is computed directly and the latter by adding zero-mean gaussian noise to the landmark points. This framework is applicable to subjective shape based biometrics.

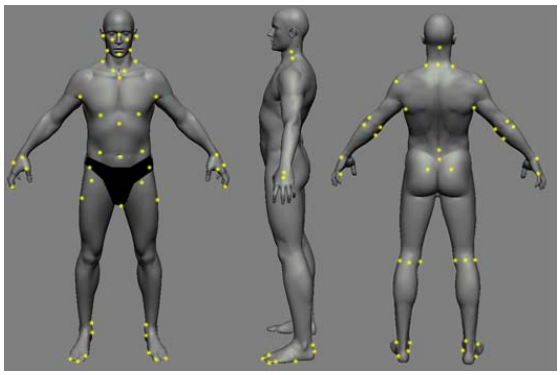

Fig. 3 Typical Caesar body and the landmark points

D. Caesar Database

The CAESAR database contains anthropometric variability of men and women, ages 18-65. High-resolution measurements of body surfaces were made using (3D) Surface Anthropometry capturing hundreds of thousands of points in three dimensions on the human body surface in a few seconds. The resulting scan is independent of the measurer, making it easier to standardize. These are point-to-point distances where the points are pre-marked by pasting small stickers on the body and automatically extracted using landmark software. The landmarks identify key bone joint structure and are adequate to segment the body and produce anatomical reference axis systems for the key body segments and joints.

III. The Asymmetry Problem and Solution

Assuming a Cartesian coordinate system, the i-th landmark point is Pi = (xi, yi, zi). The CAESAR database provides seventy-three such points for the 5000 subjects, in the three poses.

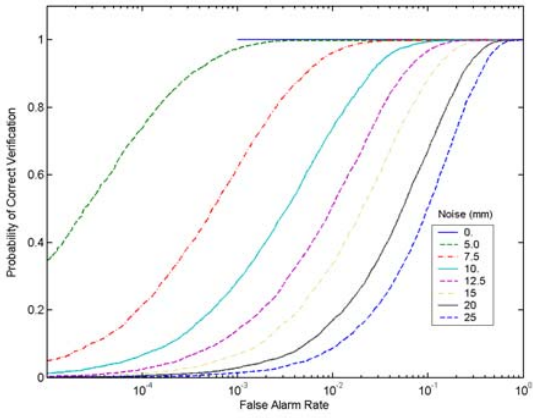

Fig. 4 Correctness Probability VS False Alarm Rate

In this study, the effect of asymmetry in human body and measurement error for biometric evaluation is compared. In this discussion, "gallery" refers to the groups of enrolled biometric signatures and "probe set" refers to the groups of "unknown" test signatures. For the gallery, the invariant segments from left part of the body and distances from the right side are used for the probe set. The recognition engine then simply computes the L1 distance between all pairs of i-th gallery and the j-th probe signatures to form the distance matrix with six, nine, and twelve segments.

It is suggested to follow the FRVT 2002 [3, 4, 5] methodology and to simply insert the original biometric vector d, from each subject into the gallery and the noise perturbed vector d' into the probe set. The resulting matrices can be used to compute the identification and erification performance scores. The standard measure of erification performance is Receiver Operating characteristic (ROC). The ROC plot shows the false alarm rate (FAR) on the horizontal axis and the probability of verification on the vertical axis, which is also one minus the false reject rate (1-FRR). FAR is the percentage of imposters wrongly accepted by the security system while FRR is the percentage of valid users rejected by the security system. Hence there will be tradeoff between FAR and FRR that depends on security policy and throughput requirements. The measure of identification performance is the "rank order statistics," called the Cumulative Match Characteristics (CMC). The rank order statistics indicate the probability that

the gallery subject will be among the top r matches to a probe. This probability depends upon both, gallery size G and r.

The feature extraction is based on the observation that humans tend to ignore isolated spots of a different color that are randomly distributed among a dominant color.

Hence, here a statistical method is proposed to identify "speckle" colors and remap them to the surrounding dominant color. As the first step we partition an image into non-overlapping NxN windows. For each window, a neighborhood color histogram matrix Hmxm is computed, where m is the number of colors found in the region. Entry H[i, j] represents the number of times that pixel with color j appears in the DxD neighborhood of a pixel with color i, divided by the total number of pixels in the DxD Neighborhoods of pixels having color i. Consequently, each row i in Hmxm represents the color histogram in the collection of neighborhoods of pixels having color i. Based on Hmxm matrix, speckle colors are detected and remapped in the following manner. For each color i, row I is examined and the entry H[i, k] that has the maximum value is found. If k equals i, then i is determined to be a dominant color, and no remapping is done. Otherwise, i is determined to be a speckle color occurring in the neighborhood of the dominant color k. Hence, all pixels with the color i are remapped to the color k. The occasional blocking effect due to windowing does not cause serious problem in this case, since images by color composition, ignored texture and edge features are compared.

IV. Pixel Comparison and Decision Making

The MFC (Most frequent color) is extracted from face region if possible or the MFC is extracted from the regions within the boundary mapped by Phase II – (Resulting regions after shape analysis). The extracted pixel set as the reference point p and comparisons are done for the range of pixels valued –p to +p, with the color in the database.

The Extracted color is negated and compared with the negative of colors in the database. This helps in extending the level of precision in comparison.

One can observe in Fig. 5 that the numbers of colors of a stream are reduced to shades of single color. For example, red, orange and brown are reduced to shades of blue. This idea can be utilized in extending the comparison precision levels to certain extent thereby reducing the color complexity in a particular region.

Fig. 5 Color Complexity Reduction through negation

V. Encryption in a SSH Data Packet

There are possibilities of overriding the control of the system. To resolve this problem it is suggested to hide the logical result by duplicating and replacing the MAC in a SSH data packet. The idea behind using a SSH packet is that the data size is not fixed and varies from 0 to 35000 octets. The intrusion may not be possible in this case nor any firewall can override this system.

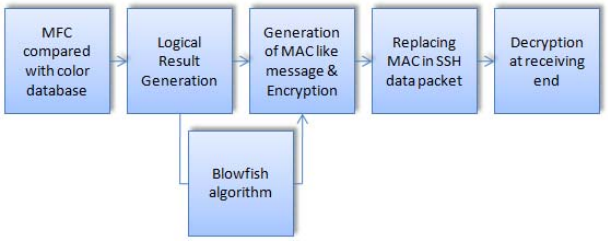

Fig. 6 Post Processes

The Initial step is to convert the logical result and replace it with the Original MAC. Algorithms like Blowfish, Twofish can generate MAC. Implementation of a Blofish is simpler and generates the Data for replacing Original MAC.

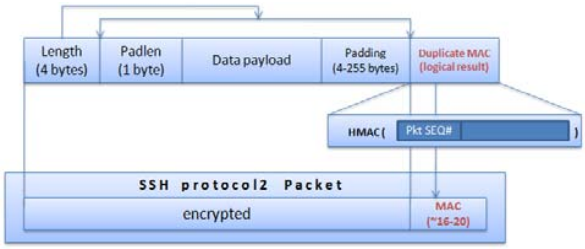

Fig. 7 SSH data Packet

VI. Generation of MAC using Blofish Cipher

Blowfish has a 64-bit block size and a variable key length from 32 up to 448 bits.[1] It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes.The diagram to the left shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

The Fig. 8 shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output.

Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. This is not so obvious because xor is commutative and associative. A common mistake is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order).

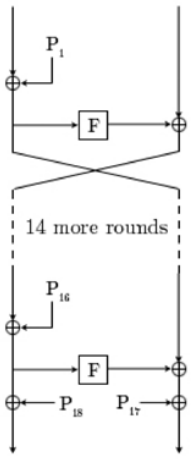

Fig. 8 Blowfish Cipher

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern (see nothing up my sleeve number). The secret key is then XORed with the P-entries in order (cycling the key if necessary). A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P1 and P2. The ciphertext is then encrypted again with the new subkeys, and P3 and P4 are replaced by the new ciphertext. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4KB of data is processed.

VII. Conclusion and Future work

The paper presents a unified approach to recognize adult images displayed in websites and to secure the results by encrypting it in a SSH data packet. It shows the usage of an alternative phase to handle failing cases such as improper face visibility. This was done in order to prevent firewalls and intrusions from overriding the control. This filter can be installed in servers that can filter the flow of data passing to the clients systems.

The theoretical data presented has been already experimented in other various applications and has been adopted by us for a different purpose. The SSH v2 is a product from free software foundation and can be deployed. The filter has been presented is designed considering both the efficiency and computational costs and robust for real time.

References

[1] Matthew A. Turk and Alex P. Pentland, "Face Recognition using Eigenfaces", *Proc. VPR*, pp. 586-591, 1991.
[2] V. I. Belhumeur, J. P. Hespanha and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 711-720, july 1997.
[3] B. J. Frey, A. Colmenarez and T. S. Huang, "Mixtures of Local Linear Subspaces for Face Recognition", *Proc. CVPR*, pp. 32-37, june 1998.
[4] B. Moghaddam, T. Jebara and A. Pentland, "Bayesian Face Recognition", Pattern Recognition, vol 33:11, pp. 1771-1782, nov 2000.
[5] G. Gordon, "Face Recognition from frontal and profile views", *Proc. Int'l Workshop on Face and Gesture Recognition*, pp. 47-52, 1996.
[6] C. Beumier and M. P. Acheroy, "Automatic Face Authentication from 3D surface", *Proc. British Machine Vision Conf. (BMVC)*, pp 449-458, 1998.
[7] Afzal Godil, Patrick Grother and Sandy Ressler, "Human Identification from body shape", *Proc. 3DIM*, pp. 386-392, oct. 2003.
[8] Alexander M. Bronstein, Michael M. Bronstein, Ron Kimmel and Alon Spira, "Face Recognition without Facial Surface Reconstruction", *Proc. ECCV*, may 2004.