

## AUTENTIFIKATSIYALASH USULLARINING SOLISHTIRMA TAHLILI

**Javlonbek Bahodir o'g'li O'ralov**

Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalar universiteti  
Urganch filiali

### ANNOTATSIYA

Ushbu maqolada ko'p foydalaniladigan biometrik autentifikatsiyalash usullarni solishtirma tahlilini amalga oshirish va aniq vazifani bajarishga mo'ljallangan axborot tizimlarini yaratishda, yuqori samara beradigan usulni taklif qilishdan iborat.

**Kalit so'zlar:** Biometrik, kaftni tanib olish, ovozni tanib olish, autentifikatsiya, yuzni tanib olish, barmoq izi, identifikatsiya, yorug'lik, shovqin, shamollash, vaqt, narx, ishonchlilik.

### **Kirish.**

Hozirgi vaqtga kelib, kompyuter-kommunikatsiya texnologiyalari kundankunga tez rivojlanib bormoqda. Shu sababli ham kompyuter texnologiyalari kirib bormagan sohaning o'zi qolmadi, desak xato bo'lmaydi. Ayniqsa ta'lim, bank, moliya tizimlarida ushbu zamonaviy texnologiyalarni qo'llash yuqori samara bermoqda. Shu bilan birga axborot havfsizligiga bo'lgan tahdid ham tobora kuchayib borayotgani hech kimga sir emas. Demak, hozirgi davrning eng dolzarb muammolardan biri axborot havfsizligini ta'minlashdan iborat.

Hozirga qadar tizimga ruxsatsiz kirishni taqiqlashning eng keng tarqalgan usuli sifatida «parol» qo'yish printsiplari hisoblanib kelmoqda. Chunki ushbu usul juda sodda, foydalanish uchun qulay va kam harajat talab etadi. Lekin, hozirga kelib «parol» tizimi to'laqonli o'zini oqlay olmayapti. Ya'ni ushbu usulning bir qator kamchiliklari ko'zga tashlanib qoldi.

### **Foydalanuvchilarni biometrik autentifikatsiyalash**

Foydalanuvchilarni biometrik autentifikatsiyalash korxonalar tashkilotining qay darajada maxfiyligi xavfsizligi jihatdan va uning iqtisod tomonlari qanchalik qoniqtira olishiga qarab biometrik autentifikatsiya qilish usullari tanlanadi. Biometrik autentifikatsiyalash usullarini muassasalarda qo'llayotgan paytda foydalanuvchi belgilarining natijalari faqat "HA" yoki "YO'Q" natijalari bilan amalga oshiriladi.[2]

### **Kaft yordamida autentifikatsiyalash.**

Kaft tanishi shaxsning qo'l geometriyasini tasdiqlaydi. Bu usul biometrik autentifikatsiyaning eng tezkor usullaridan biri va har kuni tonna mijoz to'xtab

turadigan korxonalar uchun idealdir. Barmoq izlari singari , kaftlarda tomirlarning joylashishi har bir odamda turlicha. [1]

### **Ovoz bo'yicha autentifikatsiyalash tizimlari.**

Bu tizimlarni hamma multimediyaga ega bo'lgan kompyuterlar asosida amalga oshirish mumkin. Shu sababli bu biometrik tizimlar arzonligi tarafi bilan boshqa biometrik tizimlardan ajralib turadi. Bu tizimni ishlatish uchun mikrofon yetarli .Bu tizim shaxsning tovush chastotasiga asoslanib ishlaydi.[6]

Ushbu biometrik autentifikatsiyalash usuli asosan, zamonaviy biznes markazlari ishlatiladi va ayni paytda bu texnologiya, jadal rivojlanmoqda. Ovoz bilan bir andozani qurishning ko'p yo'llari bor. Odatda, bu usul chastota va uning turli tuzilmalari va ovozli statistik xususiyatlarga ega. Shu biosdan uning muammo tomoni bir kishining ovozi xilma: ovozli salomatligi, yoshi, kayfiyat va hokazo holiga qarab farq qilishi mumkin.[5] Ushbu xilma-xillik, inson ovozi o'ziga xos xususiyatlari ajratish jiddiy qiyinchiliklar tug'diradi. Bundan tashqari, shovqin ham ovoz bilan amaliy foydalanish autentifikatsiya qilish vaqtida yana bir muhim va hal etilmagan muammo hisoblanadi.

### **Barmoq izlari yordamida autentifikatsiyalash.**

**“Barmoq izlari buyicha insonni idetifikatsiyalash”** hozirda eng keng tarqalgan usul bo'lib, axborotni himoyalash biometrik tizimlarida keng qo'llanilmoqda. Bugungi kunda 3 xil barmoq izlarini olish texnologiyasi bor ular quyidagicha:

- Ultratovushlar yordamida;
- Optik nurlar yordamida (FTIR);
- Yarim o'tkazgich yordamida; [3]

### **Yuzning tuzilishi bo'yicha autentifikatsiyalovchi tizimlar.**

Yuzning tuzilishi bo'yicha autentifikatsiya qilish hamma tamonlama ya'ni arzon va barcha kompyuterlarning video xususiyatga ega ekanligi bois bu tizim hamma joyda ishlatila olishi bilan farq qiladi. Bu tizim asosan masofaviy identifikatsiya qilish vaqtida ishlatiladi. Quyida (1-rasm) dagi nuqtalar asosida yuzning o'lchamlari hisoblanadi. Ushbu nuqtalar yuzning semirganini hisobiga ham o'zgarib turadi.Ammo yuz semirgan paytda ham ozgan paytda ham uning tuzulishi geometrik o'lchamlari va burchagi o'zgarmaydi. Bunda uning quyidagi nuqtalari o'lchamlari olinadi:

- Lab tuzilishi uning burchagi;
- Burun uchi va o'lchamlari;
- Ko'zning markazi va ko'z burchagi;

Bunda uning o'lchamlari ma'lumotlar omboridagi shaxslarning o'lchamlari bilan solishtirilib uning haqiqatda muassasada ishlaydigan shaxs yoki shaxs emasligini ko'rsatadi. Ammo bu tizimga halaqit beradigan omillar ham yetarli: Ko'zoynak, soqol, yuzga bezak berish kabilar.[4]



*1-rasm. Yuz tuzilishi bo'yicha autentifikatsiyalash.*

Rasmdagi holatda asosan ko'z, burun lab o'lchamlari olinadi va identifikatsiyalanadi.

Biometrik autentifikatsiyalash usullarning tahlil qilish jarayonida shaxsning vaqti, sog'ligi va mablag'i tomonlarni qulay bo'lishiga alohida e'tibor berilishi maqsadga muvofiq. Barmoq izi yordamida biometrik autentifikatsiya qilishda asosan uning jarohat yetmagan bo'lishi va uning skanerlash vaqtida kameraga to'g'ri qo'yilishiga, yuz yordamida biometrik autentifikatsiya qilishda yuzdagi ko'zoynak bor yo'qligi soch turmagi yuzga tushmaganligiga e'tibor qaratish lozim.[5]

### **Kaft, ovoz, yuz va barmoq izi autentifikatsiyalash usullarining solishtirma tahlili**

Biometrik autentifikatsiyalash usullarini tahlil qilish quyidagi jadval yordamida amalga oshiriladi. Ushbu jadvaldagi raqamlar ballash tizimiga asoslangan. Chunki ushbu sonlar umumiy statistikaga tayangan holda baholangan. 3 ballik tizimda xar bitta biometrik autentifikatsiyalash usulini baholab o'tamiz.

	<b>Kaft</b>	<b>Ovoz</b>	<b>Barmoq izi</b>	<b>Yuz</b>
<b>Yorug'lik</b>	3	3	3	1
<b>Shamollash</b>	3	1	3	2
<b>Shovqin</b>	3	1	3	3
<b>Ishonchlilik</b>	2	2	2	2
<b>Narxi</b>	2	3	2	3
<b>Vaqti</b>	2	2	3	2
<b>Jami</b>	<b>16</b>	<b>12</b>	<b>17</b>	<b>13</b>

Yorug'lik bo'limida autentifikatsiya qilish vaqtida kaft, ovoz hamda barmoq izi yordamida autentifikatsiyalashga hech qanday tasiri yo'qligi bois 3 ball dan baholaymiz. Yuz ordamida autentifikatsiyalashni 1 ball bilan baholaymiz chunki

yorug'lik paytida kameraga yorug'lik tushishi sababli bir qancha muammolar yuzaga kelishi mumkin.

Shamollash bo'limida autentifikatsiya qilish vaqtida kaft, barmoq izi yordamida autentifikatsiyalashga hech qanday tasiri yo'qligi bois 3 ball dan baholaymiz.

Ovoz hamda yuz yordamida biometrik autentifikatsiyalashda shamollash ovozga hamda yuzga ta'sirini ko'rsatgani bois unga 1 ball berib o'tamiz. Chunki bunday vaziyatda autentifikatsiyalashni amalga oshirishda bir qancha muammolarga duch kelamiz.[4]

Shovqinning yuzga, barmoq iziga hamda kaft yordamida autentifikatsiyalasha hech qanday ta'sir yo'qligi bois ushbu usullarga 3 ball berib o'tamiz. Ovoz yordamida biometrik autentifikatsiyalash usulini 1 ball bilan baholaymiz. Chunki shovqin vaqtida autentifikatsiyalashni amalga oshirishning bir mucha qiyin.

Ishonchlik jihatdan to'rttala autentifikatsiyalash usullariga teng 2 balldan beramiz. Chunki hozirgi kunda bularning har birini soxtalashtirish imkoniyati mavjud.[7]

Narxi jihatidan ushbu biometrik autentifikatsiyalash usullarida bir qancha farqlar borligi bois dastur va apparatning umumiy yig'insini hisobga olgan holda kaft izi va barmoq izi yordamida biometrik autentifikatsiyalash usuliga 2 ball berib o'tamiz. Ovoz va yuz yordamida biometrik autentifikatsiyalash usuliga faqatgina dasturiy vosita kerakligi va apparat kerakligi bo'lganligi bois ushbu usullarga 3 ball berib o'tamiz.

Vaqt jihatdan kaft, ovoz, yuz yordamida biometrik autentifikatsiyalash usullari 2-3 s davom etganligi sababli ularni 2 ball bilan baholaymiz va barmoq yordamida biometrik autentifikatsiyalash usuliga 3 ball berib o'tamiz.

## **Xulosa**

Olingan natijalar shuni ko'rsatadiki yuqorida keltirilgan usullarga qaraganda eng ko'p ball barmoq izi yordamida biometrik autentifikatsiyalash usuli samarali ekanligini ko'rsatdi. Uning balli 17 ball bo'lib u hamma tomonlama qulay bo'lgan, xar-hil sharoitda ham qulay va narxi ham ko'p mablag' sarf qilmaydigan usuldir.

## **FOYDALANILGAN ADABIYOTLAR**

1. G'aniev S.K., Karimov M.M. "Hisoblash sistemalari va tarmoqlarida informatsiya himoyasi": Oliy o'quv yurtlari talabalari uchun o'quv qo'llanma. - Toshkent davlat texnika universiteti, 2003.

2. A. V. Leus. Biometricheskaya autentifikatsiya po dinamicheskim xarakteristikam podpisi. Jain, A. K.; Ross, Arun & Prabhakar, Salil (January 2004), "Шаблон: Doi-inline", IEEE Transactions on Circuits and Systems for Video Technology T. 14th.

3. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems, " IBM systems Journal, vol. 40, pp. 614—634, 2001.

4. A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs, " Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, pp. 1892—1901, 2006.

5. M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, "«Corefaces»- Robust Shift Invariant PCA based Correlation Filter for Illumination Tolerant Face 68 Recognition, " presented at IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), 2004.

6. Wing (1998), —Overview of all INS Biometrics Projects, Proceedings of CTST'98, Pp. 543–552.

7. J. Markowitz (1999), —Voice Biometrics: Speaker Recognition Applications and Markets, Voice Europe 1999: European Symposium on Voice Technologies, London.